PROTECTING CHILDREN'S PRIVACY IN AN ELECTRONIC WORLD

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

OCTOBER 5, 2011

Serial No. 112–91

Printed for the use of the Committee on Energy and Commerce
energycommerce.house.gov

U.S. GOVERNMENT PRINTING OFFICE

74–138 PDF WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON ENERGY AND COMMERCE

FRED UPTON, Michigan
Chairman

JOE BARTON, Texas
Chairman Emeritus
CLIFF STEARNS, Florida
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOSEPH R. PITTS, Pennsylvania
MARY BONO MACK, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE ROGERS, Michigan
SUE WILKINS MYRICK, North Carolina
Vice Chairman
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
BRIAN P. BILBRAY, California
CHARLES F. BASS, New Hampshire
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY MCMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BILL CASSIDY, Louisiana
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. MCKINLEY, West Virginia
CORY GARDNER, Colorado
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia

HENRY A. WAXMAN, California
Ranking Member
JOHN D. DINGELL, Michigan
Chairman Emeritus
EDWARD J. MARKEY, Massachusetts
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
JANICE D. SCHAKOWSKY, Illinois
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
JOHN BARROW, Georgia
DORIS O. MATSUI, California
DONNA M. CHRISTENSEN, Virgin Islands
KATHY CASTOR, Florida

SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

MARY BONO MACK, California
Chairman

MARSHA BLACKBURN, Tennessee
Vice Chairman
CLIFF STEARNS, Florida
CHARLES F. BASS, New Hampshire
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BILL CASSIDY, Louisiana
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. MCKINLEY, West Virginia
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
JOE BARTON, Texas
FRED UPTON, Michigan *(ex officio)*

G.K. BUTTERFIELD, North Carolina
Ranking Member
CHARLES A. GONZALEZ, Texas
JIM MATHESON, Utah
JOHN D. DINGELL, Michigan
EDOLPHUS TOWNS, New York
BOBBY L. RUSH, Illinois
JANICE D. SCHAKOWSKY, Illinois
MIKE ROSS, Arkansas
HENRY A. WAXMAN, California *(ex officio)*

C O N T E N T S

PROTECTING CHILDREN'S PRIVACY IN AN ELECTRONIC WORLD

WEDNESDAY, OCTOBER 5, 2011

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 9:07 a.m., in room 2123 of the Rayburn House Office Building, Hon. Mary Bono Mack (chairman of the subcommittee) presiding.

Members present: Representatives Bono Mack, Blackburn, Harper, Lance, Cassidy, Guthrie, Olson, McKinley, Kinzinger, Barton, Butterfield, Markey, Matheson, Towns, and Waxman (ex officio).

Staff present: Andy Duberstein, Assistant Press Secretary; Kirby Howard, Legislative Clerk; Brian McCullough, Senior Professional Staff Member, CMT; Jeff Mortier, Professional Staff Member; Gib Mullan, Chief Counsel, CMT; Shannon Weinberg, Counsel, CMT; Michelle Ash, Democratic Chief Counsel, CMT; Felipe Mendoza, Democratic Counsel; and Will Wallace, Democratic Policy Analyst.

Mrs. BONO MACK. The subcommittee will now come to order.

Good morning. When it comes to online privacy protection, we have no more important job than to get it right for our kids. Today, there are an estimated 50 million children across the United States who are 13 years of age and younger. Our goal is to make sure their experiences on the Internet are as safe as possible and their privacy rights are fully protected.

And the Chair now recognizes herself for an opening statement.

OPENING STATEMENT OF HON. MARY BONO MACK, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Whether they are surfing, studying, chatting, or playing video games, kids today are spending more and more time online taking advantage of the vast, richly diverse resources found on the Internet. But as we know very well and sometimes painfully, there can be a dark side to the Internet, too. The Children's Online Privacy Protection Act was adopted by Congress in 1998 to help protect the privacy of our children. COPPA requires Web sites and other online services to obtain parental consent before collecting and sharing information from kids who are under the age of 13. As a mother and as chairman of the subcommittee, this is an issue that remains one of my top priorities, as well as one of my big areas of concern.

For the most part, the FTC has done a great job of making sure COPPA has worked well for our kids and their families, but it is time to begin asking some important questions. Should Congress revisit COPPA in light of the rapid technological advances which have been made since its enactment more than a decade ago? Is the current age threshold sufficient to protect our kids or should it be raised? If it is raised, what are the constitutional and technological implications? Is the COPPA safe harbor regime an effective self-regulatory model and could it be successfully utilized in other privacy contexts? And finally, is the expansion of the definition of personal information in the COPPA appropriate for use as a precedent in the broader online privacy context.

Today, we will begin debating these and other issues with a respected panel of experts. And one thing is very clear to me—kids today are becoming more tech savvy at a younger and younger age, but that exposure to exciting new sophisticated devices and countless Web sites located around the world doesn't necessarily mean that they are going to be able to have any better judgment or make them any more aware of what dangers might lurk online. That is why the FTC and parents everywhere must continue to play a critically important role in safeguarding the privacy of our children.

The purpose of this hearing is to take a close look at the adequacy of existing protections and whether the FTC's proposed changes to COPPA go too far, not far enough, or manage to strike the appropriate balance. Having reviewed these changes carefully, I think the FTC has, and as I often say, they have hit the sweet spot.

One of the most significant changes involves revising the definition of PII to include geolocation data and persistent identifiers such as IP addresses or device serial numbers. A second change to the existing COPPA Rule includes a new provision to govern data retention and deletion of children's PII, and it requires operators to delete information when it is no longer needed to fulfill its original purpose.

Another proposed improvement to the COPPA Rule addresses the growing unreliability of so-called "email-plus" by eliminating it as a method of parental consent. And when it comes to safe harbors, the FTC is proposing a new self-audit requirement calling for information practices to be reviewed annually. Additionally, all safe harbor programs would be required to regularly submit to the FTC the results of their annual member audits and any disciplinary actions imposed by their members.

Clearly, Chairman Leibowitz and the rest of the FTC deserve our thanks and our appreciation for conducting a careful, thorough, and thoughtful review of COPPA leading to these important recommended changes. While some privacy advocates would like to raise the COPPA age threshold because of an increasing use of social networking sites by teenagers such as Facebook, Twitter, and Google Plus, I believe the FTC showed commonsense restraint in taking a go-slow approach. The last thing we want to do is to inhibit technological advances and stifle growth of the Internet by moving forward in a new policy area without a good, smart game plan in place.

I look forward to having this particular debate in the months ahead as we continue our broader hearings on privacy. In closing, I also want to stress the importance of parental involvement in this process. It is not enough to simply check the box and provide consent. I urge all parents everywhere to regularly check out the Web sites that your kids are visiting, carefully review their privacy policies, and finally, ask questions. Make sure you clearly understand a site's practices as well as its policies and give your kids a primer on the dangers of online predators. Talk to them often and make them more self-aware. It is critically important that all of us continue to work together to keep the Internet as safe as possible for all of our children.

And now, the gentleman from North Carolina, Mr. Butterfield, the ranking member of the Subcommittee on Commerce, Manufacturing, and Trade is now recognized for his 5 minutes for his opening statement.

[The prepared statement of Mrs. Bono Mack follows:]

Opening Statement of the Honorable Mary Bono Mack
Subcommittee on Commerce, Manufacturing, and Trade
"Protecting Children's Privacy in an Electronic World"
October 5, 2011
(As Prepared for Delivery)

Whether they are surfing, studying, chatting or playing video games, kids today are spending more and more time online, taking advantage of the vast, richly-diverse resources found on the Internet. But as we know very well...sometimes painfully...there can be a dark side to the Internet, too.

The Children's Online Privacy Protection Act was adopted by Congress in 1998 to help protect the privacy of our children. COPPA requires websites and other online services to obtain parental consent before collecting and sharing information from kids who are under the age of 13.

As a mother – and as Chairman of this Subcommittee – this is an issue that remains one of my top priorities...as well as one of my big areas of concern. For the most part, the Federal Trade Commission has done a great job of making sure COPPA has worked well for our kids and their families.

But it's time to begin asking some important questions:

- Should Congress revisit COPPA in light of the rapid technological advances which have been made since its enactment more than a decade ago?
- Is the current age threshold sufficient to protect our kids or should it be raised?
- If it is raised, what are the Constitutional and technological implications?
- Is the COPPA Safe Harbor regime an effective self-regulatory model? Could it be successfully utilized in other privacy contexts?
- And, finally, is the expansion of the definition of personal information in the COPPA rule appropriate for use as a precedent in the broader online privacy context?

Today, we will begin debating these and other issues with a respected panel of experts. One thing is very clear to me: kids today are becoming more tech savvy at a younger and younger age. But that exposure to exciting, new sophisticated devices – and countless websites located around the world – doesn't necessarily mean that they are going to have any better judgment or make them any more aware of what dangers might lurk online. That's why the FTC and parents everywhere must continue to play a critically important role in safeguarding the privacy of our children.

The purpose of this hearing is to take a close look at the adequacy of existing protections, and whether the FTC's proposed changes to COPPA go too far, not far enough, or manage to strike the appropriate balance. Having reviewed these changes carefully, I think the FTC has – as I often say – hit the "sweet spot."

One of the most significant changes involves revising the definition of personal information to include geolocation data and persistent identifiers, such as IP addresses or device serial numbers.

A second change to the existing COPPA rule includes a new provision to govern data retention and deletion of children's personal information. It requires operators to delete information when it is no longer needed to fulfill its original purpose.

Another significant improvement to COPPA addresses the growing unreliability of so-called "email plus" by eliminating it as a method of parental consent.

And when it comes to Safe Harbors, the FTC is proposing a new self-audit requirement, calling for information practices to be reviewed annually. Additionally, all Safe Harbor programs would be required to regularly submit to the FTC the results of their annual member audits and any disciplinary actions imposed by their members.

Clearly, Chairman Leibowitz and the rest of the Federal Trade Commission deserve our thanks and appreciation for conducting a careful, thorough and thoughtful review of COPPA, leading to these important recommended changes.

While some privacy advocates would like to raise the COPPA age threshold because of an increasing use of social networking sites by teenagers, such as Facebook, Twitter and Google+, I believe the FTC showed common-sense restraint in taking a "go-slow" approach. The last thing we want to do is to inhibit technological advancements and stifle growth of the Internet by moving forward in a new policy area without a really good, smart game plan in place. I look forward to having this particular debate in the months ahead as we continue our broader hearings on privacy.

In closing, I also want to stress the importance of parental involvement in this process. It's not enough to simply "check the box" and provide consent. I urge all parents...everywhere...to regularly check out the websites that your kids are visiting. Carefully review their privacy policies. And, finally, ask questions. Make sure you clearly understand a site's practices as well as its policies, and give your kids a primer on the dangers of online predators. Talk to them often and make them more self-aware.

It's critically important that all of us continue to work together to keep the Internet as safe as possible for all children.

###

OPENING STATEMENT OF HON. G.K. BUTTERFIELD, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NORTH CAROLINA

Mr. BUTTERFIELD. I thank the chairman of this subcommittee and all of the others who have worked so hard to make today's hearing possible. Thank you very much because this certainly an important subject. I also want to thank the witnesses for coming forward today, and I look forward to each of your testimonies.

The privacy of our children is paramount and is an issue where we can show strong bipartisan support. Over 10 million children access the Internet on a regular basis and it is our job as policymakers to ensure that they are protected and their personal information is safe.

In 1998, consumer use of the Internet was still in its infancy. It had evolved from making about 2 percent of two-way telecommunication traffic in 1990 to over 50 percent in the year 2000. Understanding the enormity of the Internet and the pervasive effect that it would ultimately have on our daily lives, Congress passed the Children's Online Privacy Protection Act. We refer to it as COPPA. In the year 2000, the FTC COPPA Rule went into effect.

These days, homework often includes an online component. You would also find it difficult to find a child of a certain age who doesn't communicate with his or her peers over the Internet in a chat room or instant messaging program. But the majority of those Web sites children have to visit to complete schoolwork or talk to their friends require some sort of registration to use the site and service. Parents deserve to know what kind of personal information is being collected on their child and how it will be used. COPPA prohibits operators of Web sites and online services directed at children under the age of 13 from collecting personal information from them without first getting verified parental consent.

I was curious as to why a parent would give consent to have their children's information collected by an operator, and it became clear to me that even free content on Web sites has a cost. Children are avid consumers and represent a large and powerful segment of the marketplace. They spend billions of dollars a year themselves and influence others to spend billions more. Advertisers see it as an enormous opportunity to promote products and services to an eager and impressionable audience.

The FTC's proposed revised COPPA Rule addresses a number of concerns that have resulted from the technological advancements of the past 5 years. Until recently, the term geolocation didn't mean so much to the average person. Now, anyone with a GPS-enabled phone can use certain online services to broadcast their exact location to a couple of feet and anyone can see their location. Geolocation, persistent identifiers, as well as photos, videos, and audio of a child have been added to the definition of personal information. Giving Web site operators maximum latitude, the COPPA Rule requires that reasonable procedures are in place to protect the confidentiality, security, and integrity of personal information collected from children while not mandating any specific procedures or technology.

And to maximize protections for children, the FTC's proposed rule will require that Web site operators keep children's data for

only as long as absolutely necessary and that they ensure that their third-party vendors also protect children's personal data.

Now, Madam Chairman, I listened very carefully to your opening statement a moment ago and I agree with all that you said. The proposed revised COPPA Rule is stronger and it will better protect American children from their data falling into the wrong hands. It seems to me that a lot of the rules should be incorporated into the baseline privacy legislation that protects everyone, regardless of age. Someone who is 12 today and 13 tomorrow has the same privacy concerns as someone who is 18 today and 19 tomorrow. I hope that moving forward with privacy legislation we can look to COPPA's revised rule and apply the strong commonsense privacy protection measures to all Americans.

Thank you very much. I look forward to your testimony.

Mrs. BONO MACK. I thank the gentlemen.

And the Chair now recognizes the chairman emeritus of the full committee, Mr. Barton, for 1 ½ minutes.

OPENING STATEMENT OF HON. JOE BARTON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. BARTON. Thank you, Madam Chairwoman. I sincerely appreciate you holding this hearing. This is a very personal issue with me. I have been involved with privacy for a number of years and have a very special interest in children's privacy because of my 6-year-old son and my five grandchildren.

When I grew up, Madam Chairwoman, I didn't even know what a computer was. My son, though, my youngest son, 6-year-old son probably spends at least an hour a day right now playing on the computer both at school and at home. He knows better how to click on things than I do quite frankly.

As cochairman of the Privacy Caucus along with Congressman Ed Markey of this committee, I have served as a leading advocate for online consumer protection. He and I together have introduced H.R. 1895, the Do Not Track Kids Act of 2011. This legislation does five things. It updates the Children's Online Privacy Protection Act of 1998. It adds protections that children or young teenagers ages 13 to 17; it prohibits Internet companies from sending targeted advertising to children and minors; prohibits Internet companies from collecting personal and location information from anyone less than 13 years of age without parental consent and anyone less than 18 without individual consent; it would require Web site operators to develop an eraser button to give children and minors the ability to request a deletion of their personal information that they do not wish to be available on the Internet.

The issue of online privacy has become a hot topic due to the rapid growth of the Internet. I hope that this hearing, Madam Chairwoman, spotlights some of the issues and builds a bipartisan consensus to do something about it such as move the Kids Protection Act that I just mentioned. Thank you for my time and I yield back.

[The prepared statement of Mr. Barton follows:]

Opening Statement of the Honorable Joe Barton
Chairman Emeritus, Committee on Energy and Commerce
Subcommittee on Consumer, Manufacturing, and Trade
"Protecting Children's Online Privacy in an Electronic World"
October 5, 2011

Today's hearing focuses on protecting our children, and I am glad this committee is considering this issue. I want to thank the chairwoman for holding this hearing, and I would also like to welcome our panelists.

The substance of this hearing is one that I take very seriously because it is an issue that is personal to me. I am the proud father of a six-year old son named Jack, and like most children these days, he spends a good amount of his free time playing video games on our home computer. When I think about my own childhood experiences, playing around on a computer never comes to mind; however, children are now increasingly exposed to the dangers of the internet world by their increased activity online.

As a co-Chairman of the Bi-Partisan Privacy Caucus, I serve as an advocate and leading voice for online consumer protection. I have introduced H.R. 1895, the Do Not Track Kids Act of 2011 with my friend from across the aisle Mr. Markey. This legislation does five important things:

1. Updates the Children's Online Privacy Protection Act of 1998 (COPPA) to make the act applicable to advanced mobile technologies and applications;

2. Adds protections to those ages 13-17,this is called the "Digital Marketing Bill of Rights for Teens," and it reinforces protections for those 12 and under;

3. Prohibits internet companies from sending targeted advertising to children and minors;

4. Prohibits internet companies from collecting personal and location information from anyone less than 13 years of age without parental consent and anyone less than 18 without individual consent. This prohibition is designed to prevent internet companies from developing online profiles of children; and

5. Requires website operators to develop an "eraser button" method to give children and minors the ability to request a deletion of all of their personal information they do not wish to be available on the internet, to the extent technologically feasible.

The issue of online privacy protection has become a hot topic due to the rapid growth of the internet. I think that we all can agree that the internet has become a driving force in this country, and as of March 2011, there are an estimated 2.1 billion users worldwide. With more people using the internet, there are more opportunities for personal information to be misused, and I believe that all Americans should have a choice in how their personal information is handled.

With that Mr. Chairman, I yield back.

Mrs. BONO MACK. I thank the gentleman.

The Chair now recognizes Mr. Olson from Texas for 1 minute.

OPENING STATEMENT OF HON. PETE OLSON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. OLSON. I thank the Chair for holding this important hearing as we continue our discussions about online privacy issues.

As a father of a 14-year-old daughter and 11-year-old son, nothing is more important to me than keeping my kids safe. Kids today, like mine, have access to new technologies that enable them to get online instantly from almost anywhere and access and share information. Congress recognized there was a need to protect children's Internet privacy and enacted the Children's Online Privacy Protection Act, COPPA, in 1998. As we examine the FTC's proposed changes to the COPPA Rule, we need a clear understanding of all the tools currently available to parents to protect their children's privacy on the Internet before we determine what changes are needed to COPPA. We cannot legislate in search of a problem.

I thank the witnesses for being here and look forward to the hearing. I yield back.

Mrs. BONO MACK. I thank the gentleman and now will recognize the ranking member of the full committee, Mr. Waxman, for 5 minutes for his opening statement.

OPENING STATEMENT OF HON. HENRY A. WAXMAN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. WAXMAN. Thank you, Madam Chair.

In 1998, thanks to the leadership of Representative Ed Markey and Dr. Kathryn Montgomery, Congress passed and President Clinton signed the Children's Online Privacy Protection Act, and today, we are fortunate to have Dr. Montgomery back before the committee to talk about this landmark law and her recommendations for the future.

I am pleased that 11 years after enactment, your overall assessment is that COPPA is a "clear legislative success." COPPA has withstood the test of time, which is remarkable because innovation occurs at warp speed online. One reason for its success is that it was written to be flexible. The law gives the Federal Trade Commission the authority and the discretion to carry out several broad mandates aimed at protecting young children from the unfair collection and use of their information.

The last several years in particular have been a period of rapid change in the delivery of online services. Young children now have access to social networks, interactive gaming, and apps on mobile devices that they carry with them everywhere they go. The FTC is responding to these developments by using its authority to update the COPPA Rule so that the law remains an effective tool for protecting children's privacy and safety.

The updates to the COPPA Rule proposed by the FTC are appropriate, reasonable, well -hought-out, and true to the intent of the law. These changes will ensure that parents of young children will remain in control of their information, whether it be their precise location at any given time, their photographic images, or a record

of their online habits and activities. That is consistent with the goal of the law—that parents, not businesses, get to decide what information about their children can and should be revealed online.

While the focus of this hearing is children's privacy, we must not forget that adults need privacy protections, too. People of all ages need more control over their information and better privacy protection. I have said this before and I will say it again. We should enact comprehensive privacy legislation. Next week's privacy hearing will be our fourth this year. There were six privacy hearings in the last Congress. Each hearing has made me more and more convinced that current law does not ensure proper privacy protections for consumer information.

As we consider comprehensive legislation, there are some clear lessons to be drawn from the 11 years of privacy protection for young children under COPPA. First, it is possible to provide consumers with real, enforceable online privacy protections without killing innovation on the Internet; and second, it is possible to craft legislation in such a way that the direction from Congress is precise and clear, but the authority of the agency is flexible enough to adapt to changes in technology and changes in social expectations and behavior. Those are valuable lessons. I hope they will be remembered when hopefully comprehensive privacy legislation is considered by this committee.

Thank you, Madam Chair, and I am going to yield back the balance of my time.

[The prepared statement of Mr. Waxman follows:]

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED TWELFTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115

Majority (202) 225–2927
Minority (202) 225–3641

Opening Statement of Rep. Henry A. Waxman
Ranking Member, Committee on Energy and Commerce
Hearing on "Protecting Children's Privacy in an Electronic World"
Subcommittee on Commerce, Manufacturing, and Trade
October 5, 2011

In 1998, thanks to the leadership of Representative Ed Markey and Dr. Kathryn Montgomery, Congress passed and President Clinton signed the Children's Online Privacy Protection Act.

Today, we are fortunate to have Dr. Montgomery back before the Committee to talk about this landmark law and her recommendations for the future. I am pleased that 11 years after enactment, her overall assessment is that COPPA is a "clear legislative success."

COPPA has withstood the test of time, which is remarkable because innovation occurs at warp speed online. One reason for its success is that it was written to be flexible. The law gives the Federal Trade Commission the authority and the discretion to carry out several broad mandates aimed at protecting young children from the unfair collection and use of their information.

The last several years in particular have been a period of rapid change in the delivery of online services. Young children now have access to social networks, interactive gaming, and "apps" on mobile devices that they carry with them everywhere they go. The FTC is responding to these developments by using its authority to update the COPPA rule so that the law remains an effective tool for protecting children's privacy and safety.

The updates to the COPPA rule proposed by the FTC are appropriate, reasonable, well thought-out, and true to the intent of the law. These changes will ensure that parents of young children remain in control of their information, whether it be their precise location at any given time, their photographic images, or a record of their online habits and activities. That is consistent with the goal of the law: that parents, not businesses, get to decide what information about their children can and should be revealed online.

While the focus of this hearing is children's privacy, we must not forget that adults need privacy protections too. People of all ages need more control over their information and better privacy protection.

I have said this before; we should enact comprehensive privacy legislation. Next week's privacy hearing will be our fourth this year. There were six privacy hearings in the last Congress. Each hearing has made me more and more convinced that current law does not ensure proper privacy protections for consumer information.

As we consider comprehensive legislation, there are some clear lessons to be drawn from the 11 years of privacy protection for young children under COPPA. First, it is possible to provide consumers with real, enforceable online privacy protections without killing innovation or the Internet. Second, it is possible to craft legislation in such a way that the direction from Congress is precise and clear, but the authority of the agency is flexible enough to adapt changes in technology and changes in social expectations and behavior.

Those are valuable lessons and I hope they will be remembered when hopefully comprehensive privacy legislation is considered by this Committee.

Thank you.

Mrs. BONO MACK. I thank the gentleman and I look forward to our continued work together on privacy.

And now I would like to turn our attention to the panel. We have just one panel of witnesses today joining us. Each of our witnesses has, as usual, prepared an opening statement that will be placed into the record. Each of you will have 5 minutes to summarize the statement in your remarks.

On our panel we have Mary Koelbel Engle, Associate Director, Division of Advertising Practices at the Federal Trade Commission. Also testifying is Hemanshu Nigam, Founder and Chief Executive Officer of SSP Blue. Next is Morgan Reed, Executive Director, Association for Competitive Technology. Our fourth witness is Stephen Balkam, Chief Executive Officer of the Family Online Safety Institute. Our fifth witness is Dr. Kathryn Montgomery, Director of the Ph.D. Program at the School of Communication at the American University. And our final witness is Alan Simpson with Common Sense Media.

Good morning and thank you all very much for coming. You will each be recognized for 5 minutes. To help you keep track of time, there are the lights in front of you as is standard. You know what yellow, green, and red each mean. As it turns yellow either hit the gas or slam on the brakes. You get to decide. And please just make sure you turn on your microphone before you begin. And Ms. Engle, you may start for your 5 minutes.

STATEMENTS OF MARY KOELBEL ENGLE, ASSOCIATE DIRECTOR, DIVISION OF ADVERTISING PRACTICES, FEDERAL TRADE COMMISSION; HEMANSHU NIGAM, FOUNDER AND CHIEF EXECUTIVE OFFICER, SSP BLUE; MORGAN REED, EXECUTIVE DIRECTOR, ASSOCIATION FOR COMPETITIVE TECHNOLOGY; STEPHEN BALKAM, CHIEF EXECUTIVE OFFICER, FAMILY ONLINE SAFETY INSTITUTE; KATHRYN C. MONTGOMERY, DIRECTOR, PH.D. PROGRAM, SCHOOL OF COMMUNICATION, AMERICAN UNIVERSITY; AND ALAN SIMPSON, VICE PRESIDENT OF POLICY, COMMON SENSE MEDIA

STATEMENT OF MARY KOELBEL ENGLE

Ms. ENGLE. Good morning, Chairman Bono Mack, Ranking Member Butterfield, and members of the subcommittee. My name is Mary Engle, and I am the associate director for advertising practices in the Bureau of Consumer Protection at the Federal Trade Commission. I appreciate the opportunity to appear before you today to discuss the Commission's enforcement and administration of the Children's Online Privacy Protection Act—or COPPA—Rule.

Congress enacted COPPA in 1998 to address the unique privacy and safety risks created when young children under the age of 13 access the Internet. The goals of the act were to limit the online collection of personal information from children without their parents' permission to protect children's safety when they view and post information online and to maintain the confidentiality and security of personal information that is collected from children.

The Commission believes that COPPA has largely worked well to fulfill these purposes and that even as online practices evolve, the law remains important today. The Commission has brought 17 ac-

tions to enforce COPPA since the COPPA Rule went into effect garnering more than $16.2 million in civil penalties. Our cases, which have been against both large, established operators, and smaller or newer companies often illustrate different core provisions of COPPA.

For example, as social networking Web sites exploded onto the youth scene about 5 years ago, the Commission sought to ensure that these sites understood their COPPA obligations. In 2006, the Commission obtained a then-record civil penalty of $1 million against Xanga.com, a popular social networking site that allegedly improperly registered 1.7 million child users without first obtaining their parents' permission. Since then, the Commission has brought a steady stream of cases against operators such as Sony BMG Music Entertaining, Iconix Brand Group, and Playdom Incorporated, each of whom sought to engage child users in the Web 2.0 world. The Commission's $3 million civil penalty against Playdom set a new record for COPPA cases.

More recently, in the first COPPA case involving mobile applications, the Commission charged mobile app developer W3 Innovations with violating COPPA by collecting and maintaining personal information from thousands of children and allowing them to publicly post personal information on in-app message boards for their Dress-Up and Girl World games. This case, which included a $50,000 civil penalty made clear that COPPA reaches mobile online services and not just traditional online services and Web sites.

Although law enforcement is a critical part of the Commission's COPPA program, enforcement alone cannot accomplish all of the agency's goals. The Commission also works to educate businesses and consumers about their rights and responsibilities under the law. The agency devotes significant resources to assisting Web site operators with rule compliance, regularly updating business education materials, and responding to inquiries from operators and their counsel. The Commission's consumer education materials, including our online safety portal OnGuardOnline.gov, inform parents and children about the Rule's protections and also provide them with general online privacy and safety information.

To help ensure that COPPA continues to work well, especially in the face of an explosion of children's mobile devices and interactive online services, the Commission initiated a review of the COPPA Rule last year. Drawing from the expertise the agency has gained in enforcing and administering COPPA over the years and after extensive consideration of public input, last month, the Commission proposed modifications to certain areas of the COPPA Rule.

While the Commission's testimony goes into these changes in greater detail, among the proposed changes are updating the Rule's definition of personal information to include geolocation information and the use of persistent identifiers to direct online behavioral advertising to children, improvements to the notices that operators must use to inform parents of the operator's information collection practices, the addition of a number of permissible methods operators may use to obtain parental consent, strengthening the Rule's data security protections, ensuring of agency oversight of the COPPA Safe Harbor Programs. The proposed changes are consistent with the original mandates in the COPPA statute. The

Commission will take public comments on these proposals until November 28.

The Commission takes seriously the challenge to ensure that COPPA continues to meet its originally stated goals even as children's interactive media use moves at warp speed. Thank you for this opportunity to discuss the Commission's COPPA program, and I look forward to your questions.

[The prepared statement of Ms. Engle follows:]

PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION

ON

"Protecting Children's Privacy in an Electronic World"

Before the

HOUSE COMMITTEE ON ENERGY AND COMMERCE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING AND TRADE

Washington, D.C.

October 5, 2011

I. Introduction

Chairman Bono Mack, Ranking Member Butterfield, and members of the Subcommittee, my name is Mary Engle, and I am the Associate Director for Advertising Practices of the Bureau of Consumer Protection at the Federal Trade Commission ("Commission").[1] I appreciate the opportunity to appear before you today to discuss the Commission's regulatory review of the Children's Online Privacy Protection ("COPPA") Rule.[2]

The Federal Trade Commission has long been committed to helping to create a safer, more secure, online experience for children. In the eleven years since the COPPA Rule first became effective, the Commission has actively engaged in law enforcement as well as business and consumer education to promote knowledge of, and adherence to, COPPA. As the members of this subcommittee are aware, in light of rapidly evolving technology and changes in the way children use and access the Internet, the Commission initiated a comprehensive review of the COPPA Rule last year. The purpose of this review was to ensure that the Rule was keeping pace with changes in the marketplace, and that it was fulfilling its statutory mandate without imposing undue burdens. The COPPA review was launched as a part of a broader Commission effort that, since 1992, has involved the systematic and rigorous review of rules to ensure that they are still necessary and are appropriately balanced. In addition, this year, the Commission committed to an aggressive schedule of regulatory reviews and has sought public comment to improve its

---

[1] While the views expressed in this statement represent the views of the Commission, my oral presentation and responses to questions are my own and do not necessarily reflect the views of the Commission or any individual Commissioner.

[2] The Commission's COPPA Rule was promulgated pursuant to the Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506. The text of the COPPA Rule can be found at 16 C.F.R. Part 312.

regulatory review program.[3]

This testimony first provides a brief legislative and regulatory overview of the COPPA statute and Rule. It next summarizes the Commission's efforts to enforce the COPPA Rule and to educate businesses and consumers about the law. Finally, it discusses the proposed changes to the Rule that the Commission announced in mid-September.

II. A Brief COPPA Overview

A. The Legislation

Congress enacted the COPPA statute in 1998 to address the unique privacy and safety risks created when young children – those under 13 years of age – access the Internet. The goals of the Act were to: (1) enhance parental involvement in children's online activities in order to protect children's privacy; (2) protect children's safety when they visit and post information on public chat rooms and message boards; (3) maintain the security of children's personal information collected online; and (4) limit the online collection of personal information from children without parental consent.[4]

COPPA applies to operators of websites and online services directed to children under age 13, and to other operators that have actual knowledge that they are collecting personal information from such children (collectively, "operators"). The statute generally mandates that operators covered by the Act provide notice of their information collection practices and, with only limited exceptions, obtain verifiable parental consent *prior* to the collection, use, or

---

[3] *See* Press Release, Federal Trade Commission, FTC Enhances Longstanding Regulatory Review Program to Increase Public Participation and Reduce Burden on Business (July 7, 2011), *available at* http://www.ftc.gov/opa/2011/07/regreview.shtm.

[4] *See* 144 Cong. Rec. S11,651 (Oct. 7, 1998) (Floor Statement of Sen. Bryan, co-sponsor of the Act).

disclosure of personal information from children. Operators also must give parents the opportunity to review and delete personal information their children have provided. Operators are required to establish and maintain reasonable procedures to protect the security of personal information collected from children, and must not condition children's participation in website activities on the disclosure of more personal information than is reasonably necessary.[5] COPPA contains a safe harbor provision enabling industry groups or others to submit to the Commission for approval self-regulatory guidelines to implement the statute's protections.[6]

B. The Commission's COPPA Rule

The COPPA statute mandated that the Commission promulgate and enforce regulations to implement the Act. The Commission's COPPA Rule became effective on April 21, 2000,[7] and the Rule closely follows the statutory language. COPPA authorizes the Commission to enforce the Rule in the same manner as it does rules promulgated under Section 18(a)(1)(B) of the Federal Trade Commission Act prohibiting unfair or deceptive acts or practices.[8] This permits the Commission to obtain civil penalties against operators who violate the Rule. While COPPA does not grant a private right of action, the statute authorizes state attorneys general to enforce compliance with the Rule by filing actions in federal court with written notice to the Commission.[9]

---

[5] 15 U.S.C. §§ 6502(b)(1)(C), 6502(b)(1)(D).

[6] 15 U.S.C. § 6503.

[7] 16 C.F.R. § 312 (2011).

[8] 15 U.S.C. §§ 6502(c), 6505(a), (d); 15 U.S.C. § 57a(a)(1)(B).

[9] 15 U.S.C. § 6504. To date, only Texas has filed law enforcement actions under COPPA. *See* News Release, "Attorney General Abbott Takes Action Against Web Sites That

III. The Commission's COPPA Enforcement and Education Efforts

A. Enforcing COPPA

The Commission believes that companies take their obligations under COPPA seriously. Nevertheless, the Commission has found law enforcement actions a useful aid in improving compliance. Thus, in the eleven years since the Rule's enactment, the Commission has brought seventeen COPPA enforcement actions that serve COPPA's core goals – ensuring that parents are informed and have the opportunity to say "no" before their young children divulge their personal information online. This requirement is especially important when, with the mere touch of a screen or the click of a mouse, a child's personal information can be collected and viewed by anyone. Together, the Commission's actions have garnered more than $6.2 million in civil penalties.[10]

Over the past five years, as social networking exploded onto the youth scene, the Commission has sought to target the wide array of new products and services offered to children online. In 2006, the Commission obtained a then-record civil penalty of $1 million against Xanga.com, a popular social networking site alleged to have knowingly collected personal information from, and created blog pages for, 1.7 million child users – without first obtaining their parents' permission.[11]

Since then, the Commission has brought a steady stream of cases against operators

---

Illegally Collect Personal Information from Minors," (Dec. 5, 2007), *available at* http://www.oag.state.tx.us/oagNews/release.php?id=2288.

[10] News releases detailing each of the Commission's 17 COPPA cases are available at http://business.ftc.gov/legal-resources/30/35.

[11] *United States v. Xanga.com, Inc.*, No. 06-CIV-6853 (S.D.N.Y., Sept. 11, 2006) (consent decree).

seeking to engage children in the Web 2.0 world. In December 2008, Sony BMG Music Entertainment agreed to pay a $1 million civil penalty to resolve allegations that the company knowingly and improperly collected a broad range of personal information from at least 30,000 children who registered on 196 of its general audience music fan sites.[12] In 2009, Iconix Brand Group, Inc., the owner and marketer of several apparel brands popular with children and teens, agreed to pay a $250,000 penalty for allegedly collecting and storing personal information from approximately 1,000 children, and for allegedly enabling girls to share personal stories and photos publicly online on one of the sites, without first notifying their parents or obtaining parental consent.[13]

In May of this year, the Commission settled charges against Playdom, Inc., a leading developer of online virtual worlds, and its principal, who were alleged to have collected from and disclosed personal information (such as full names, email addresses, instant messenger IDs, and locations) of hundreds of thousands of children who registered on Playdom sites. The Commission's $3 million civil penalty set a new record for COPPA cases.[14]

Most recently, in the Commission's first COPPA case involving mobile applications, the Commission charged mobile app developer W3 Innovations, LLC with violating COPPA by collecting and maintaining thousands of girls' email addresses, and also allowing girls to publicly post information, including personal information, on in-app message boards for their

---

[12] *United States v. Sony BMG Music Entertainment*, No. 08 Civ. 10730 (S.D.N.Y, Dec. 15, 2008) (consent decree).

[13] *United States v. Iconix Brand Group, Inc.*, No. 09-CV-8864 (S.D.N.Y., Nov. 5, 2009) (consent decree).

[14] *United States v. Playdom, Inc.*, No. SA CV-11-00724 (C.D. Cal., May 24, 2011) (consent decree).

"dress up" and "girl world" apps.[15] This case, which included a $50,000 civil penalty, made clear that COPPA reaches mobile online services and not just traditional websites.

B. Business and Consumer Education

Although law enforcement is a critical part of the Commission's COPPA program, enforcement alone cannot accomplish all of the agency's goals in this arena. A crucial complement to the Commission's formal law enforcement efforts, therefore, is educating businesses and consumers about their rights and responsibilities under the law. By promoting business and consumer education, the Commission seeks to help the greater online community create a culture that protects children's privacy and security.

The Commission's business outreach goals focus broadly on shaping prospective practices. The agency devotes significant resources to assisting website operators with Rule compliance, regularly updating business education materials and responding to inquiries from operators and their counsel.[16]

The Commission's consumer education materials inform parents and children about the protections afforded by the Rule and also provide them with general online privacy and safety information. The Commission's consumer online safety portal, OnGuardOnline.gov, provides information in a variety of formats – articles, games, quizzes, and videos – to help consumers

---

[15] *United States v. W3 Innovations, LLC*, No. CV-11-03958 (N.D. Cal., Sept. 8, 2011) (consent decree).

[16] To facilitate COPPA compliance, the Commission maintains a comprehensive children's privacy section of its online Business Center. *See* http://business.ftc.gov/privacy-and-security/children%E2%80%99s-online-privacy. In addition, the FTC staff provides individual website operators with fact-specific guidance on COPPA issues as they arise through phone calls placed to the FTC's COPPA Hotline.

guard against Internet fraud, secure their computers, and protect their personal information.[17] In 2008, Congress directed the FTC to expand OnGuardOnline.gov to cover online safety for children. The agency responded by developing a guide for parents, *Net Cetera: Chatting with Kids About Being Online*, as well as the *Net Cetera Community Outreach Toolkit* to help people share the *Net Cetera* information.[18]

IV. The Current Regulatory Review

A. Background

In 2005, the Commission commenced a statutorily required review of its experience in enforcing COPPA and the Rule.[19] After completing that review, the Commission concluded that there was a continuing need for COPPA's protections, and that the Rule should be retained without change.[20] At that time, however, the Commission also acknowledged that children's

---

[17] Currently, 16 federal agencies are partners on OnGuardOnline.gov, contributing content and helping to promote and disseminate consistent messages. OnGuardOnline attracts approximately 100,000 unique visitors each month.

[18] *See* OnGuardOnline, "Net Cetera: Chatting With Kids About Being Online," *available at* http://onguardonline.gov/sites/default/files/articles/pdf/NetCetera_ChattingwithKids.pdf. *Net Cetera* focuses on the importance of communicating with children about cyberbullying, sexting, social networking, mobile phone use, and online privacy. The Commission has distributed more than 8.5 million English language, and over 900,000 Spanish language, copies of the guide since it was introduced in October 2009. The FTC has distributed almost 40,000 Net Cetera Community Outreach Toolkits to community-based organizations around the country since it was introduced in October 2010.

[19] In particular, the statute and the Rule mandated that the FTC's review address the Rule's effect on three issues: (1) operators' practices relating to the collection, use, and disclosure of children's information; (2) children's ability to obtain access to information of their choice online; and (3) the availability of websites directed to children. *See* 15 U.S.C. § 6507; 16 C.F.R § 312.11.

[20] *See* Children's Online Privacy Protection Rule, 71 Fed. Reg. 13,247 (Mar. 15, 2006) (retention of COPPA Rule without modification). The Commission reported to Congress

growing embrace of mobile Internet technology and interactive general audience sites, including social networking sites, without the concomitant development of suitable age verification technologies, presented challenges for COPPA compliance and enforcement.[21]

Although the Commission generally reviews its rules on a rotating ten-year calendar, the continued rapid-fire pace of technological change, including an explosion in children's use of mobile devices and participation in interactive online services, led the agency to accelerate its subsequent review of COPPA. Accordingly, in April 2010, the Commission published a Federal Register Notice seeking public comment on whether technological changes to the online environment over the preceding five years warranted any changes to the Rule.[22] The Commission's request for public comment examined each aspect of the COPPA Rule, posing 28 questions for the public's consideration.[23] In June 2010, the Commission held a public roundtable to discuss in detail several areas where public input was sought,[24] and the comment period closed in mid-July 2010.

In addition to the dialogue at the public roundtable, the Commission received 70

---

on the results of its COPPA review in 2007. *See* Fed. Trade Comm'n, *Implementing the Children's Online Privacy Protection Act: A Report to Congress* (2007), *available at* http://www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf.

[21] *See Implementing the Children's Online Privacy Protection Act*, *id.* at 28-29.

[22] *See* Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule ("2010 Rule Review"), 75 Fed. Reg. 17,089 (Apr. 5, 2010), *available at* http://www.ftc.gov/os/fedreg/2010/april/P104503coppa-rule.pdf.

[23] *Id.*

[24] Information about the June 2, 2010 COPPA Roundtable is available at http://www.ftc.gov/bcp/workshops/coppa/index.shtml.

comments from industry representatives, advocacy groups, academics, technologists, and individual members of the public. The comments addressed the efficacy of the Rule generally, and several possible areas for change, as discussed further below.[25]

B. The Commission's Proposed Rule

After extensive consideration, the Commission recently proposed modifications to the Rule in five areas: Definitions, Notice, Parental Consent, Confidentiality and Security of Children's Personal Information, and Safe Harbor Programs.[26] In addition, the Commission proposed adding a new Rule section addressing data retention and deletion. This testimony will provide an overview of the principal changes, which are intended to update the Rule to meet changes in technology, assist operators in their compliance obligations, strengthen protections over children's data, and provide greater oversight of COPPA safe harbor programs. All of these proposed changes are to the Commission's Rule and are consistent with the original mandates in the COPPA Act. The Commission will take public comments on this proposal until November 28, 2011. The Commission expects to hear from a wide variety of stakeholders during this time; often, the Commission makes changes to an initial proposal based on the public comments.

1. Definitions

a. Personal Information

COPPA requires operators to obtain verifiable parental consent before collecting personal information from children online. The COPPA statute defines "personal information"

---

[25] The public comments in response to the Commission's April 5, 2010 Federal Register Notice are available at http://www.ftc.gov/os/comments/copparulerev2010/index.shtm.

[26] The Commission's Notice of Proposed Rulemaking can be found at 76 Fed. Reg. 59,804 (Sept. 15, 2011), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-09-27/pdf/2011-24314.pdf.

as individually identifiable information about an individual collected online, and lists a set of identifiers deemed by Congress to be personal, including "any other identifier that the Commission determines permits the physical or online contacting of a specific individual."[27] Based on this statutory authority, the FTC proposes to update the Rule's definition of personal information as follows:

First, the Commission proposes adding to the list persistent identifiers (*e.g.*, numbers held in cookies, user IDs, IP addresses, processor or device serial numbers, or unique device identifiers), as well as screen and user names, where they are used for functions other than "support for the internal operations of a site or service."[28] The Commission also proposes including as "personal information" other identifiers that link a child's activities across different sites or services.[29] The effect of these additions would be to require parental notification and consent prior to the collection and use of persistent identifiers for purposes such as behaviorally targeting advertising to a child, while permitting operators' use of persistent identifiers for purposes such as user authentication, improving site navigation, maintaining user preferences, serving contextual advertisements, protecting against fraud or theft, and other activities necessary to maintain the technical functioning of a site or service.[30] While the Commission is

---

[27] 15 U.S.C. § 6501(8)(F).

[28] *See* Notice of Proposed Rulemaking, *supra* note 26, at 59,812.

[29] *Id.*

[30] Behavioral advertising is the tracking of a consumer's online activities over time – including the searches the consumer has conducted, the web pages visited, and the content viewed – in order to deliver advertising targeted to the individual consumer's interests. *See FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising*, at 52 (Feb. 2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf. Contextual advertising is advertising based on a consumer's current visit to a single web page or a single search query

not aware of any operator directing online behavioral advertising to children, the Commission hopes to obtain further information during the comment period.

Second, the Commission proposes adding to the definition of "personal information" geolocation information sufficient to identify street name and name of city or town. In the Commission's view, any geolocation information that provides precise enough information to identify the name of a street and city or town already is covered under the existing Rule.[31] Nevertheless, because geolocation information may be presented in a variety of formats (*e.g.*, coordinates or a map), and in some instances may be more precise than street name and name of city or town, the Commission proposes making geolocation information a stand-alone category within the Rule.[32]

Finally, given the prevalence and popularity of posting photos, videos, and audio files online, the Commission has reexamined the privacy and safety implications of such practices as they pertain to children. Inherently, photos can be very personal in nature and may, in and of themselves, contain information, such as embedded geolocation data, that permits physical or online contacting. In addition, new facial recognition technologies can be used to further identify persons depicted in photos. Therefore, the Commission proposes that, with respect to the subset of websites and online services directed to children or having actual knowledge of collecting personal information from children, the Rule cover as "personal information" photos,

---

that involves no retention of data about the consumer's online activities beyond that necessary for the immediate delivery of an ad or search result. *Id.* at 5.

[31] *Id.* at 59,813.

[32] *Id.*

videos, and audio files containing children's images or voices.[33] The effect of this proposal would be to require verifiable parental consent prior to allowing children to upload such files on COPPA-covered websites or online services.

b. Collects or Collection

The Commission also proposes to amend the Rule's definition of "collects or collection" that currently exempts an operator from COPPA's requirements if it is able to delete *all* individually identifiable information from postings by children before they are made public, and also deletes such information from its records.[34] This provision, which has come to be known as the "100% deletion standard," often serves as an impediment to operators' implementation of sophisticated filtering technologies that might aid in the detection and removal of personal information. In its place, the Commission proposes a "reasonable measures" standard whereby operators who employ technologies reasonably designed to capture *all or virtually all* personal information inputted by children will not be deemed to have "collected" personal information.[35] This proposed change is intended to encourage the development of systems, either automated, manual, or a combination thereof, to detect and delete, prior to its public posting, all or virtually all personal information that children may submit.

2. Parental Notification

The linchpins of the COPPA Rule are its parental notice and consent requirements. Providing parents with clear and complete notice of operators' information practices is the

---

[33] *Id.*

[34] 16 C.F.R. § 312.2.

[35] *See* Notice of Proposed Rulemaking, *supra* note 26, at 59,808.

necessary first step in obtaining informed consent from parents. COPPA requires that parents be notified in two ways: (1) on the operator's website or online service (the "online notice," which typically takes the form of a privacy policy); and (2) in a notice delivered directly to a parent whose child seeks to provide personal information on the site or service (the "direct notice"). The current Rule requires that operators provide extensive information about their information collection practices pertaining to children in their online notice. While the Rule states that the direct notice must contain the information an operator includes in its online notice as well as certain additional information, the Commission previously has indicated that operators may truncate the information in the direct notice by providing a hyperlink to their online privacy policy.[36]

The Commission proposes changes to streamline and clarify these notices. Outside of the COPPA context, the Commission recently has begun to urge industry to provide consumers with notice and choice about information practices at the point consumers enter personal data or before accepting a product or service.[37] The analogous point of entry under COPPA would be the direct notice, which has the potential to provide parents with the best opportunity to consider an operator's information practices and to determine whether to permit their children to engage with such operator's website or online service. Therefore, the Commission proposes to revise the notice requirements to reinforce COPPA's goal of providing complete and clear information

---

[36] *See* Children's Online Privacy Protection Rule, 1999 Statement of Basis and Purpose, 64 Fed. Reg. 59,888, 59,897 (Nov. 3, 1999), *available at* http://www.ftc.gov/os/1999/10/64Fr59888.pdf.

[37] *See A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* 57-59 (Dec. 1, 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf;

in the direct notice, and to rely less heavily on the online notice as the means of providing parents with information about operators' information practices.[38]

First, the Commission proposes specifying, for each different form of direct notice required by the Rule, the precise information that operators must provide to parents. The Commission also proposes that each form of direct notice provide a hyperlink to the operator's online notice of information practices. The Commission believes these changes will help ensure that parents receive key information up front, while directing them online to view any additional information contained in the operator's online notice.

Second, with respect to the content of the online notice, the Commission proposes eliminating the Rule's current lengthy recitation of an operator's information collection, use, and disclosure practices in favor of a simple statement of: (1) what information the operator collects from children, including whether the website or online service enables a child to make personal information publicly available; (2) how the operator uses such information; and (3) the operator's disclosure practices for such information.[39] In the Commission's experience, privacy policies are often long and difficult to understand, and may not be the most effective way to communicate salient information to consumers, including parents.[40] By proposing to streamline the Rule's online notice requirements to reflect the basic language of the COPPA statute, the Commission seeks to encourage operators to provide clear, concise descriptions of their information practices. This should have the added benefit of being easier to read on smaller

---

[38] *See* Notice of Proposed Rulemaking, *supra* note 26, at 59,815.

[39] This language mirrors the statutory requirements for the online notice. *See* 15 U.S.C. 6502(b)(1)(A)(i).

[40] *See Protecting Consumer Privacy in an Era of Rapid Change*, *supra* note 37, at 7.

screens (*e.g.*, those on Internet-enabled mobile devices) by the very parents who need to receive such information.

3. Parental Consent

A central element of COPPA is its requirement that operators seeking to collect, use, or disclose personal information from children first obtain verifiable parental consent. The Rule provides that operators "must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology," and that "any method to obtain verifiable parental consent must be reasonably calculated in light of available technology to ensure that the person providing consent is the child's parent."[41] To aid operators, the Rule then sets forth a non-exclusive list of methods that meet the standard of verifiable parental consent.[42]

The Commission proposes several changes to the mechanisms of verifiable parental consent. First, the Commission proposes expanding the list of approved mechanisms by adding electronic scans of signed parental consent forms, video conferencing, and use of government-issued identification checked against a database (provided that the parent's ID is deleted promptly after verification is completed).[43]

Second, the Commission proposes eliminating the Rule's sliding scale, or "email plus," approach to parental consent. Under the sliding scale, an operator, when collecting personal information only for its *internal* use, may obtain verifiable parental consent through an email from the parent, so long as the email is coupled with an additional step. Such additional steps

---

41 16 C.F.R. § 312.5(b)(1).

42 16 C.F.R. § 312.5(b)(2).

43 *See* Notice of Proposed Rulemaking, *supra* note 26, at 59,818.

have included: obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call, or sending a delayed confirmatory email to the parent after receiving consent.[44] When the Commission issued the original COPPA Rule in 1999, it provided for the email plus option to sunset after two years, out of recognition, expressed by many businesses, that email plus is not as reliable as the other enumerated methods of verifiable parental consent.[45] The Commission found this lower cost method acceptable as a temporary option, in place *only* until the Commission determined that more reliable (and affordable) consent methods had adequately developed.[46]

While email plus has enjoyed wide appeal among operators, who commend its simplicity, many commenters challenged the method's reliability.[47] The Commission believes that the continued reliance on email plus has inhibited the development of more reliable methods of obtaining verifiable parental consent.[48] In addition, although internal uses may pose a lower

---

[44] 16 C.F.R. § 312.5(b)(2).

[45] *See* 1999 Statement of Basis and Purpose, *supra* note 36, at 59,902.

[46] *Id.* at 59,901. In 2002, the Commission extended the use of the email plus option for an additional three years when more reliable methods of parental consent had not developed. *See* Children's Online Privacy Protection Rule, 67 Fed. Reg. 18,818, 18,819-21 (Apr. 17, 2002). In 2006, the Commission extended use of the sliding scale indefinitely, stating that the agency would continue to monitor technological developments and modify the Rule should an acceptable electronic consent technology develop. *See* Children's Online Privacy Protection Rule, 71 Fed. Reg. 13,247, 13,254-55 (Mar. 15, 2006) (retention of Rule without modification).

[47] In particular, commenters noted that operators have no real way of determining whether the email address provided by a child is that of the parent, and that there is no requirement that the parent's email response to the operator contain any additional information providing assurance that it is from a parent. *See* Notice of Proposed Rulemaking, *supra* note 26, at 59,819, n.153.

[48] *Id.*

risk of misuse of children's personal information than the sharing or public disclosure of such information, *all* collection of children's personal information merits effective verifiable parental consent. Indeed, the COPPA statute does not distinguish between the types of parental consent required for internal versus external uses of children's personal information.[49] In light of this, the Commission believes that email plus has outlived its usefulness and should no longer be a recognized approach to parental consent under the Rule.[50]

In the interest of spurring innovation in parental consent mechanisms, and to promote greater flexibility for operators, the Commission proposes adding two new consent processes in place of email plus: (1) establishing a voluntary 180-day notice and comment process whereby parties may seek Commission approval of a particular consent mechanism; and (2) permitting operators participating in a Commission-approved safe harbor program to use any parental consent mechanism deemed by the safe harbor program to meet the Rule's general consent standard.[51]

4. Data Security, Retention, and Deletion

To better protect children's personal information, the Commission proposes strengthening the Rule's security requirements in several ways. First, it proposes adding a requirement that operators take reasonable measures to ensure that any service provider or third party to whom they release children's personal information has in place reasonable procedures to

---

[49] *See* 15 U.S.C. § 6502(b)(1)(A)(ii). Instead, that distinction was created by the Commission when it promulgated the COPPA Rule. *See* 16 C.F.R. § 312.5(b)(2).

[50] *See* Notice of Proposed Rulemaking, *supra* note 26, at 59,819.

[51] *Id.* at 59,820.

protect the confidentiality, security, and integrity of such personal information.[52] Second, the Commission proposes adding a provision requiring operators to retain children's personal information for only so long as is reasonably necessary, and to properly delete such information by taking reasonable measures to protect against unauthorized access to, or use of, the data in connection with, its disposal.[53]

5. Safe Harbor Programs

The COPPA statute established a "safe harbor" for participants in Commission-approved COPPA self-regulatory programs.[54] The safe harbor provision was designed to encourage industry members and other groups to develop their own COPPA oversight programs, thereby promoting efficiency and flexibility, and rewarding operators' good faith efforts to comply. The Rule therefore provides that operators fully complying with an approved safe harbor program will be "deemed to be in compliance" with the Rule. In lieu of formal enforcement actions, such operators instead are subject first to the safe harbor program's own review and disciplinary procedures.[55] Currently, there are four Commission-approved COPPA safe harbor programs.[56]

---

[52] *Id.* at 59,821.

[53] *Id.* at 59,822.

[54] 15 U.S.C. § 6503.

[55] *See* 16 C.F.R. §§ 312.10(a) and (b)(4).

[56] Since the Commission's COPPA Rule took effect on April 21, 2000, four groups have received Commission approval of their safe harbor programs: the Children's Advertising Review Unit of the National Advertising Division of the Council of Better Business Bureaus, the Entertainment Software Rating Board, TRUSTe, and Privo, Inc. Another safe harbor application, that of Aristotle International, Inc., currently is pending before the Commission. For information on the safe harbor process, see http://business.ftc.gov/privacy-and-security/children%E2%80%99s-online-privacy/safe-harbor-program.

The Commission proposes three substantive changes to strengthen the safe harbor provision while retaining the elements that make this self-regulatory scheme effective: (1) requiring that applicants seeking Commission approval of self-regulatory guidelines submit comprehensive information about their capability to run an effective safe harbor program; (2) establishing more rigorous baseline oversight by Commission-approved safe harbor programs of their members; and (3) requiring Commission-approved safe harbor programs to submit periodic reports to the Commission. The purpose of these proposed changes is to enable the Commission to better evaluate safe harbor applications, and to improve the accountability and transparency of COPPA safe harbor programs that have been approved. At the same time, the changes to the consent mechanisms, discussed above, would provide greater flexibility to such programs as they develop their requirements and manage compliance.

V. Conclusion

The Commission takes seriously the challenge to ensure that COPPA continues to meet its originally stated goals, even as children's interactive media use moves and changes at warp speed. Thank you for this opportunity to discuss the Commission's COPPA program and our proposed updates to the Rule. I look forward to your questions.

Mrs. BONO MACK. Thank you very much, Ms. Engle.
Mr. Nigam, you are recognized for 5 minutes.

STATEMENT OF HEMANSHU NIGAM

Mr. NIGAM. Chairman Bono Mack, Ranking Member Butterfield, and members of the subcommittee, thank you for giving me the opportunity to provide insight on best ways to protect children's privacy in an electronic world.

I have been at the forefront of nearly every major aspect of online and offline child safety for the past 20 years. Today, I am the founder and CEO of SSP Blue, a safety, security, and privacy strategic business consulting firm. My company provides strategic guidance that promotes the protection of consumers, especially children, encourages corporate social responsibility, and develops partnerships with law enforcement, government, and NGOs. Past and current clients have included News Corporation, Microsoft, AT&T, Tagged, Formspring, and others. To be clear, I do not speak on behalf of any of our existing clients today.

Prior to SSP Blue, I served in leadership roles at News Corporation, MySpace, Microsoft, and MPA from the time the Internet was just a baby to the time that social media was barely a toddler, and in each endeavor, I provided strategic direction that put children's safety, security, and privacy at the forefront of the business. I have also served as a federal prosecutor against Internet crimes against children and computer crimes at the Justice Department, an advisor to the COPPA Commission, and advisor to the White House Committee on Cyberstalking, and as a prosecutor against child molestation and sex crimes in the L.A. County District Attorney's Office.

And so I speak to you from various perspectives in government, in law enforcement, in private industry, and as a father of four children ranging in age from 6 to 16.

The FTC has engaged in a meticulous and thoughtful process in the review of the Child Online Privacy Protection Act and should be congratulated. I also want to stress a concept that is easily forgotten. The industry has an incentive to do the right thing when it comes to protecting children's privacy rights. Businesses lose when they violate a child's privacy rights. Their brand reputation suffers, their consumer loyalty drops, their friends in child advocacy groups disappear, and most important, they lose the trust of the parents and guardians who care for the very children that they cater to. In essence, without doing the right thing, an online business cannot succeed.

Within this context, I would like to propose this subcommittee a framework on how we should approach whether and what changes are needed in COPPA. Whenever we think of protecting children, whether it is for their safety, security, or privacy, our first inclination is to protect them from anything that sounds bad instead of what is bad. Solutions based on things that sound bad eventually will fail. In the past 10 years, I have had the honor of advising the COPPA Commission, sitting on the Berkman Center Internet Safety Technical Taskforce, and co-chairing the federal Online Safety Working Group. In each of these endeavors, we could have responded to problems that sounded bad, and instead, we spent the

time finding the actual problems and then proposing the necessary solutions.

While technologies have evolved since the advent of COPPA, I urge you to consider whether an actual problem has been clearly articulated that needs to be solved when looking at each individual change that is being proposed. Next, consider whether existing regulations can be used to respond to an identified problem. Looking back on the FTC's COPPA enforcement actions, it is clear that current regulations and rules have been quite useful and effective. In fact, a great majority of the industry does a tremendous job in working within the rules, whether their product is directed at children under 13 or 13 and over. Even new companies know what is expected of them before they enter the marketplace. Interestingly, companies are finding it easier to provide services for the 13-plus as a much better business model.

And so we must ask whether today there are other bad actors the FTC finds it cannot enforce against as an evolving landscape created gaps. In areas where existing regulations are needed, we should then determine the best solution. Several factors should be considered. What we must ask: 1) Would the proposed change actually close an identified gap? 2) Would it create technical implementation challenges? 3) Would it lead to conflicted with other agency and department demands or expectations such as conflict that arises between data retention, data minimization, and data preservation? And 4) Would it lead to unintended consequences such as creating disincentives to providing a rich online experience for the under-13?

If we utilize this framework when considering the changes, I think we will be able to protect children's online privacy by implementing solutions that work while the technology evolves.

And in closing, I want to stress that if we were to accept the proposed changes in whole, we can expect an immediate impact on the marketplace. Larger companies will adjust where they can and simply shut down areas where there is simply too much uncertainty. And smaller and newer companies will find investors spooked by uncertainties. Such a multi-year cycle can be avoided if you spend the time now to examine the proposal within the framework that we are outlining and identify actual problems, create effective solutions that can be readily implemented by those already incentivized to do the right thing.

Thank you, Chairman Bono Mack, Ranking Member Butterfield, and members of the subcommittee, for giving me this opportunity to address you on this important topic.

[The prepared statement of Mr. Nigam follows:]

PREPARED STATEMENT OF HEMANSHU NIGAM
FOUNDER AND CEO, SSP BLUE

"PROTECTING CHILDREN'S PRIVACY IN AN ELECTRONIC WORLD"

THE SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE
OF THE HOUSE ENERGY AND COMMERCE COMMITTEE

UNITED STATES HOUSE OF REPRESENTATIVES
2123 Rayburn House Office Building

Washington, D.C.
October 5, 2011

Chairman Bono Mack, Ranking Member Butterfield, and members of the Subcommittee, thank you for giving me the honor of appearing before you today to provide insight on the best ways to protect children's privacy in an electronic world.

I have been at the forefront of nearly every major aspect of offline and online child safety for the past 20 years. Today, I am the founder and CEO of SSP Blue, a safety, security, and privacy strategic business consulting firm for online businesses. My company provides clients with strategic guidance on creating an online presence that protects their consumers, promotes corporate social responsibility, and engages in partnerships with government, law enforcement, and NGOs. Past and current clients have included News Corporation, Microsoft, AT&T, Tagged, Formspring, and others. To be clear, I do not speak on behalf of any of our existing or past clients.

Prior to SSP Blue, I served as News Corporation and MySpace's Chief Security Officer when social media was barely a toddler. Prior to that, I worked inside Microsoft Corporation to set in motion a cross-company strategy for child safe computing and led a cyber security enforcement

team. Before Microsoft, I was Vice President of Worldwide Internet Enforcement against digital movie piracy at the Motion Picture Association of America. I have also served as a federal prosecutor against Internet child exploitation and computer crimes at the U.S. Department of Justice, an advisor to the COPA Commission, and an advisor to the White House's Committee on Cyberstalking. Finally, I began my career as a prosecutor in the LA County District Attorney's office, specializing in child molestation and sex crimes cases.

And so, I speak to you from various perspectives in private industry, government, and law enforcement, and as a father of four children ranging in age from 6 to 16.

I want to first praise the work of the Federal Trade Commission for its meticulous and thoughtful approach in reviewing the Child Online Privacy Protection Act ("COPPA") to identify areas of improvement.

As a backdrop, I also want to stress a concept easily forgotten. The industry has an incentive to do the right thing when it comes to protecting children's privacy rights. Businesses lose when they are accused of violating a child's rights – their brand reputation suffers, their consumer loyalty drops, their friends in child advocacy groups disappear, and most important, they lose the trust of the parents and guardians who care for the very children they cater to. In essence, doing the right thing is synergistic with the short and long-term viability of a business – with survival.

Within this context, I would like to provide this Subcommittee a framework on how we should approach whether changes are needed in COPPA and what they should be.

Whenever we think of protecting children, whether it is for their safety, security, or privacy, our first inclination is to protect them from anything that sounds 'bad' instead of just what is 'bad'. Solutions based on things that sound bad eventually fail. In the past ten years, I've had the honor

of advising the COPA Commission, sitting on the Berkman Center Internet Safety Technical Task Force, and co-chairing the Online Safety Working Group. In each endeavor, we could have taken the easy way out by offering a myriad of solutions in response to problems that sounded bad. Instead, we focused on identifying whether and what the problem is that we needed to solve. Only then did we articulate necessary solutions.

While technologies may have evolved since the advent of COPPA, I urge you to consider whether an actual problem has been clearly articulated that needs to be solved when looking at each individual change that is being proposed.

Next consider whether existing regulations can be used to respond to an identified problem. Looking back on the FTC's COPPA enforcement actions, it is clear that current regulations have been quite useful and effective. In fact, a great majority of the industry does a tremendous job in working within the framework and guidelines whether their product is directed at minors under 13 or 13 and over. Even new companies know what is expected of them before they enter the marketplace. Interestingly, companies find providing services to 13 plus a much better business model.

We must ask whether there are today other bad actors that the FTC finds it cannot enforce against. Has the evolving landscape created gaps? In some areas the answer is yes and in some areas perhaps no.

In areas where existing regulations needed to be adjusted, we should then determine what the best solution would be. Several factors will affect the outcome. We must ask whether the proposed change:

1. would actually close an identified gap

2. create technical implementation challenges especially given the multitude of products and business models that often exist inside a single company
3. lead to conflicts with other agency and department demands or expectations that are just as legitimate such as the conflict that arises between date retention, minimization, and preservation, or
4. lead to unintended consequences such as creating disincentives to providing rich online experiences for the under 13 members of our digital society.

If we can utilize this framework when considering the proposed changes, I think we will be able to protect our children's privacy by implementing solutions that work in an ever evolving interconnected world.

I do want stress that if we are to accept all the changes proposed, we can expect an immediate impact on the marketplace:

1. Larger companies will try to adjust to the changes, implementing fixes where they can and shutting off areas where too much uncertainty lies;
2. Smaller Companies seeking venture capital investments will find it harder to obtain funding in the face of unclear paths to defendable implementations.

That said, as with any new regulations, once they are tested and clarified, the industry will eventually feel more confident to invest again. But, such a cycle can be avoided if we spend the time to examine the proposals within the framework I have outlined above.

In closing, I want to stress the importance of protecting children's privacy in today's electronic world. Our task is to do it in a way that responds to clearly identified problems with effective

solutions that can be properly implemented by those who are already incentivized to do the right thing.

Thank you Chairman Bono Mack, Ranking Member Butterfield, and members of the Subcommittee for giving me this opportunity to address you on this important topic.

////

Mrs. BONO MACK. Thank you very much.
Mr. Reed, you are recognized for 5 minutes.

STATEMENT OF MORGAN REED

Mr. REED. Chairman Bono Mack, Congressman Butterfield, thank you for holding this important hearing on children's privacy, FTC, and COPPA regulations. My name is Morgan Reed and I am with the Association for Competitive Technology, and we represent the mobile apps developers. With more than 3,000 members spread throughout the United States and the world, our folks are focused on doing all those cool apps you see on television.

So during the past year, ACT has had a chance to reach out to our developers and other developer organizations throughout America to discuss privacy and the importance of privacy by design. At a recent conference, I was scheduled to present on privacy, but before I spoke, developers were given an opportunity to talk about their business. Everyone got up and said this is what they were excited about, this is the direction their business was going, and as I heard all these folks talk, I noticed at the end of their conversation always concluded with two words. And these two words are two words we don't hear much in the United States right now and they are words that I think are absolutely critical to all of our discussions going forward. Those two words—"We're hiring."

And the good news is this wasn't just some random event that I was at where it was a special enclave of jobs that no one knows about. A recent study out of the University of Maryland shows that Facebook apps alone have created 200,000 jobs. Our own internal studies show that 600,000 jobs have been created, saved, or supplemented from the mobile apps economy. And the good other part of this news is is that with all deference to Chairman Bono Mack's great State of California, 88 percent are small businesses and over 70 percent are not in the great State of California. So it is widespread, it is small, and it is growing.

Now, besides creating jobs, developers as a community are passionate about one other thing and that is privacy. And education apps are particularly focused on privacy because the vast majority of mobile apps are built by parents. Now, these aren't folks who started their company looking to get rich; they were looking to provide an interactive family experience for their kids on this device that they brought home from work.

So they want to do good and that is why we are working with organizations like PrivacyChoice.org to build privacy policy generators so that they can easily become aware of and comply with privacy regulations. But before we all get into the specifics about Section 312.4 of the NPRM or what the meaning of "collect" is, I thought I would take some time to discuss the kinds of apps these small developers are creating.

For example, from your district we have Animal Apps and Animal Pronunciations from Palm Springs. For Congressman Butterfield's district, we have got We Pray, Pray With Me, which is a special app for the iPad that allows grandparents to record a prayer for their child so that if they are aware, if they are out of state, if they can't see them, the child can hear their voice. It is

also used by parents that are deployed overseas and folks who are just on business trips. What a great app.

We have got from Congressman Waxman's district, we have got 3 Trees, which helps educate kids about water, sun, and air, and the three elements that power the world. From Congressman Lance's district, we have got Random Acts of Kindness, which helps kids know about 300 different random acts of kindness they can do, charities they can donate to, and inspiration for goodwill. From Utah, we have Tap Fuse. They have got two great apps—one that helps kids with the alphabet; another that they are doing right now that is about anti-bullying. Congressman Harper, Mississippi State currently offers field studies in iPhone entrepreneurship at Mississippi State and right now you have got one guy out of there who is still a freshman, his app has already sold 20,000 copies and it is an education app for kids in school.

Congressman Guthrie, we have got Oink-a-Saurus, which is a great app. It is a piggy bank that helps kids learn about the stock market and how they can save money. Congressman Olson, we have got Music Master, high tech flashcards for practicing reading music. In Maryland, we have got Pickpocket Books, which was a company built by a woman literally a stay-at-home mom on her couch who watched her child using the iPad and said, you know, I would like to combine this technology with my child's love of reading. Since then, she has built a micro empire of more than 80 books on the iPad store that she has hired voice actors, artists, and developers who have created interactive applications that allow children to listen to the book, have the book read to them, and read back and practice.

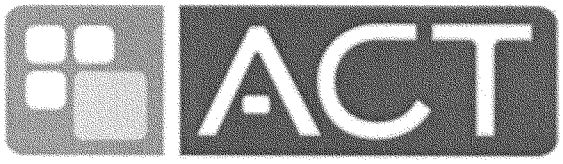
Now, my own daughter who is now 5–3/4 she reminds me likes math apps from Montessorium from Sioux Falls, South Dakota. It is a great app that combines the tactile Montessori Method of teaching with the touch pad on an iPad screen.

Now, I know that some here will talk about those in the tech industry or media in a way that implies the larger faceless corporation. I love the FTC's testimony earlier but she said we speak with the companies and their counsel. The vast majority of companies that I have named have no in-house counsel right now, and so for them this is a learning process.

Now, I want you to remember that the incredible innovation happening today is not driven by faceless corporations but by thousands of moms and dads working to build applications that educate, motivate, and enrich their families. So let us make sure that we don't mess up this as we work to achieve a better online privacy protection.

Thank you for your time and I look forward to your questions.

[The prepared statement of Mr. Reed follows:]



Testimony

of
Morgan Reed
Executive Director
The Association for Competitive Technology

before the
House Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing and Trade

on
Protecting Children's Privacy in an Electronic World

October 5, 2011
2123 Rayburn House Office Building

Chairman Bono Mack, Ranking Member Butterfield, and distinguished members of the Committee: My name is Morgan Reed, and I would like to thank you for holding this important hearing on children's online privacy and the proposed changes to COPPA.

I am the executive director of the Association for Competitive Technology (ACT). ACT is an international advocacy and education organization for people who write software programs--referred to as application developers--and providers of information technology (IT) services. We represent over 3,000 small and mid-size IT firms throughout the world and advocate for public policies that help our members leverage their intellectual assets to raise capital, create jobs, and innovate.

My goal today is to help explain how small businesses that are fueling explosive growth in the mobile apps marketplace have become aware of their responsibilities under COPPA, how the rule changes outlined in the FTC's Notice of Proposed Rulemaking (NPRM) may affect them, and how small businesses are attempting to meet the goals of COPPA through innovation and parental outreach.

Overall, app developers have three key messages for members of this committee:

1. **The mobile apps ecosystem is creating American jobs and innovative new products but heavy-handed new regulations could threaten that success.**
2. **The NPRM demonstrates the power and the flexibility of the original COPPA legislation, and proves that technology-specific privacy legislation is unwarranted at this time.**
3. **The NPRM does a good job of clarifying and modernizing the original COPPA regulations. However, there are still areas where we think the FTC needs to expand examples of what is permissible and pull back from changes that could limit innovation.**

The Smartphone Ecosystem is Creating Jobs and Opportunities in a Tough Economy

The evolution of mobile technology has led to a renaissance in the software industry; small software companies that once wrote exclusively for big software platforms at the enterprise level are now able to create innovative products and sell them directly to consumers. The emergence of the app market is a radical departure from the era of up-front marketing costs, publisher delays, and piracy. Its growth has eliminated the longstanding barriers to

entry that our industry battled for the past two decades.

In the face of this tough economic environment, there has been a bright spot in the: sales of smartphones and tablets, such as the iPhone, the HTC Thunderbolt (running Google Android) the Samsung Focus (running Microsoft WP7), the iPad, Xoom and Amazon's "Fire" continue to outpace all predictions and are providing a huge growth market in a slumping economy. Nearly one hundred million smartphones were shipped in the first quarter of 2011[1] marking a 79% increase in an already fast growing market.[2] In fact, 40% of adult mobile phone owners in the United States have smartphones. At the end of last year, smartphone sales were 20% of the U.S. market. Europe now sells more smartphones than feature phones[3].

In 2008 Apple launched its App Store to provide a place for developers to sell independently developed applications for the iPhone. Since then, over 500,000 new applications have gone on sale, with billions of applications sold or downloaded. The Android platform has recently exceeded the growth rate seen in the iPhone, totaling more than 300,000 applications. In 2010 we saw the release of Windows Phone 7 with its own applications store and an entirely unique user interface. Just last week, Microsoft released "Mango", and Amazon launched the "Fire" tablet. Total unique apps across all platforms are expected to hit one million by the end of 2011,[4] and the future looks bright.

The Mobile App World – A Job Growth Engine

The mobile app marketplace has grown to a five billion dollar industry from scratch in less than four years. In the next four, analysts expect that number to reach $38 billion -- exceeding $54 billion when including service expenditures[5].

A recent study by the University of Maryland found the Facebook platform for app developers has created more than 182,000 jobs generating over $12 billion in wages and benefits.[6] Facebook is just one platform that app

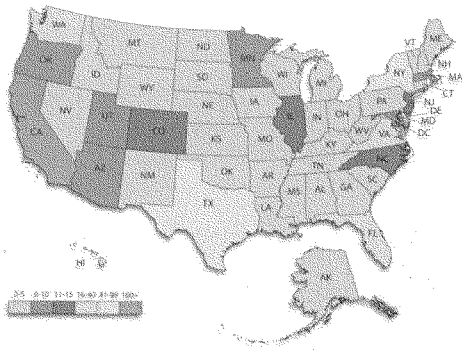
[1] Mark Kurlyandchik, *IDC: Nokia Remains Top Smartphone Vendor Worldwide*, DailyTech, May 6, 2011.
[2] *Id.*
[3] http://www.engadget.com/2011/09/12/smartphones-out-ship-feature-phones-in-europe-samsung-leads-the/
[4] http://d2omthbq56r2fx.cloudfront.net/wp-content/uploads/2011/04/Distimo-survey-201103-app-stores-count.png
[5] http://blogs.forrester.com/john_mccarthy/11-02-28-mobile_app_internet_making_sense_of_the_2011_mobile_hysteria
[6] http://www.rhsmith.umd.edu/digits/pdfs_docs/research/2011/AppEconomyImpact091911.pdf

developers write for, with iOS, Android, and Windows Phone 7 also attracting mobile app developers. ACT's own research estimates that the current mobile apps economy has created, saved or supplemented more than 600,000 jobs nationwide.

ACT regularly conducts workshops for app developer groups throughout the country and we hear about opportunity for jobs in the app development world. And these aren't just programmer jobs; app developers often need graphic artists, content writers and marketers to assist in app development.

The jobs created by app development are not just in Silicon Valley. During the dot-com years, the majority of growth occurred in the California while the rest of the country was not able to reap the direct benefits of the economic boom. However, today's mobile apps industry is experiencing job creation across the country.

App Developers Across the Country



While California continues to have a large representation of app developers, nearly 70% of the businesses are located outside of the state of California. The nature of this industry allows developers to live almost anywhere, including: *Animal's Pronunciations A to Z* by Rickety Apps in California, *Otto the Otter* by Baked Ham Games in North Carolina, and *Christ Church United Methodist* app by Speak in Tennessee.

Another feature of this new industry is that small businesses are the driving economic force. Of the 500 best-selling mobile apps, 88% are produced by small businesses.[7] In a majority of cases these are micro businesses with less than 10 employees.

[7] ACT analysis of top 500 selling apps, some discrepancies exist due to lack of verifiable employment data and apps created by a developer who has significant investment from a larger company. Some apps branded for a larger company are in fact developed by small firms subcontracted to build the application. Sample size of 408 applications, from "top apps" on March 25 2011.

The Power of the FTC to Protect Children

The FTC has been aggressive in utilizing the power of existing COPPA regulations. The app community has drawn particular attention as the Commission has recently focused on a few bad apples operating without regard for COPPA. Through actions both big (Playdom, $3 million fine) and small (W3, $50,000 fine) the Commission's enforcement actions have raised awareness in the apps community that COPPA applies to them. Despite evidence to the contrary, some critics believe the FTC does not have the tools necessary to protect children in today's online world. This is clearly not the situation.

Recent steps taken have shown the Commission is effectively identifying and addressing the problems of bad actors in the industry. Moreover, FTC's rulemaking authority provides flexibility so that COPPA may be updated when necessary as evidenced by the most recent proposed changes.

These concerns are reflected in the FTC's position on proposed legislation: it has consistently denied new laws are necessary. When FTC Chairman Leibowitz testified before the Senate Committee On Commerce, Science, and Transportation, he noted the Commission needs no new laws.[8] Again, in testimony before Senators Rockefeller and Kerry in the Senate Commerce Committee, the FTC made clear its position that it already possesses sufficient regulatory tools to address privacy online and in the mobile marketplace, including for children. Rather than new legislation, the FTC continues to point out the need for more resources to increase the number and effectiveness of their enforcement actions.

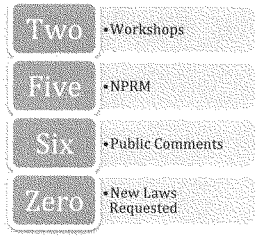
The FTC's NPRM Shows the Power to Adapt COPPA to Technology – Some lawmakers want to put new legislation's cart before the FTC's NPRM horse. Most recently in HR 1895, the "Do Not Track Kids Act", the Bill's authors propose amendments to COPPA that seek to address issues already covered by the FTC's latest NPRM.

[8] For now, FTC Chairman Jon Leibowitz is willing to give the industry a chance before calling for legislation. Even without a government mandate, he noted, it's in the industry's self-interest to make Do Not Track work. After all, Leibowitz says, "nobody wants to be on the wrong side of consumers." Jolee Tessler, *Internet privacy controls challenge tech industry*, Bloomberg Businessweek (July 26, 2011).

A cursory review of the NPRM shows multiple examples:

- Section 3 of HR 1895 requires clear and conspicuous notice to children; addressed by the NPRM
- Section 3 expands COPPA to cover "Apps"; again, this is in the NPRM
- Section 6 requires express authorization prior to collection of geo-location from minors. The NPRM already covers this for under 13. Moreover, this seems to be after-the-fact as all the smartphone platforms are providing notification and an opt-in requirement when the GPS is initially activated by an app.

In 11 Years the FTC Has Updated COPPA Via:



Therefore, Congress should let the FTC make the adjustment to the existing COPPA regulations before proposing new legislation.

How the NPRM Effectively Updates COPPA

The FTC has taken affirmative steps to update COPPA to changes in the technology marketplace. Clarifying and modifying existing law, this latest NPRM offer guidance to help app developers create quality content for children while protecting children's privacy.

Maintaining Consistency in the Age of Applicability - The FTC wisely maintained the existing age of COPPA applicability to those under 13. While the increasing of the COPPA age to 17 and under as some have requested, would likely be found unconstitutional,[9] it would also upset the framework on which much of the Internet is based.

For example, many general audience Internet sites that collect personal information do not allow users under 13. If forced to comply with COPPA retroactively due to an increase in age, many users might suddenly find their access revoked. This could include access to cloud-based storage of their personal documents, social networking sites, and even sites as innocent as MovieFone and WashingonPost.com.

[9] *See Ashcroft v. American Civil Liberties Union*, 542 U.S. 656 (2004) (upholding the injunction of enforcement of COPA due, in part, to its applicability to those under 18).

Increased Clarity on COPPA's Application to Apps – The NPRM removes any uncertainty for mobile app developers about the applicability of COPPA and clarifies some key terms. While undefined by the original COPPA language, the NPRM provides certainty to identify apps as an "online service." This helps us in our educational outreach efforts to increase awareness among our members of the need to comply with COPPA and to inform how they achieve compliance.

Increased Parental Notice is a Good Thing - We believe that transparency to the consumer is critical. Transparency informs consumers of how their information is being collected and used. This allows consumers to make educated decisions while eliminating the "scary factor." ACT has been very active communicating to our developers about the need to create and use privacy policies if their app collects personal information.

We do worry, however, that requiring too much disclosure produces unnecessary burdens on developers while not providing appreciable benefits to consumers. Still, we are pleased to see the FTC's emphasis on empowering consumers to make informed decision with greater transparency.

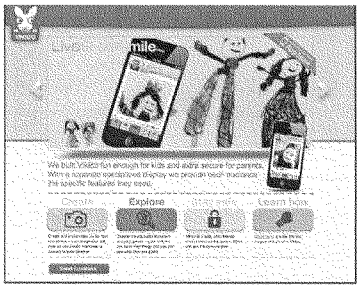
COPPA is aimed at protecting children's privacy online while increasing parental notice, consent, and involvement in how and when a child can share their information online. As app developers, this is also at the heart of the apps that we develop for children.

The FTC Should Encourage Innovation in Parental Consent – Parental engagement is necessary for truly effective COPPA compliance and appears to be the goal of the statute. We want parents to know what their child shares online and we want them to be involved. But when the FTC considers completely removing systems like email plus, it only discourages websites and developers from creating engaging, useful tools for children. This is especially the case when, as the FTC states, "few, if any, new methods for obtaining parental consent have emerged since the sliding scale was last extended in 2006."[11] Alternative email verification services will not arise because of stricter COPPA guidelines – instead, we need to find ways to make parental consent easier. That means not letting the perfect become the enemy of the good. We believe the FTC should re-examine elimination of email plus to

[11] COPPA Rule Review, 16 CFR Part 312, Project No. P104503 p. 64 (FTC Notice of Proposed Rulemaking 2011).

determine if there are other ways to encourage innovation, including investigating alternative systems that are part of social network sites, game systems, and global marketplaces.

App Developers are innovating to Obtain Parental Consent and Provide Notice - COPPA compliance is an incredible hurdle faced by small mobile app developers – who are challenged by screen size, business size, and



evolving business models. The good news is we are innovating. Take for example the app developer Vikido. Vikido's mantra is "Create, Explore, Stay Safe." Children's safety is at the core of the Vikido application, highlighted from the very first screen on. Vikido allows children to share pictures and statements online, but only after first obtaining parental consent through Facebook Connect. Vikido's privacy policy clearly states that no information from the child will be shared except through the parent account, and they've taken the time to explain COPPA to parents directly in their blog:

> ***So, What is Vikido doing about this?***
>
> 
>
> *We started Vikido as "concerned parents" and that is why kids on Vikido don't have an "account" in the regular sense of the word – it's an extension of the parent's account. The parent logs in using FB connect, creates a "child" account – and the child is logged-in only via the parent's permissions – entering a child-mode interface.*
>
> *So – no one can connect with your child unless you approve it (you add a family member via YOUR parent side, but the child doesn't have this ability).*
>
> *In addition, no one can see the child's feed (other than his family) and the only person who can share the child's creations is the parent. You can see an example on my own facebook account: https://www.facebook.com/amit.knaani/posts/10150310197421443 - that's me as a parent, sharing my child's pic under my name.*
>
> *We also added an additional level of control by notifying the parent when a message is sent to the child.*
>
> ***"But it's kind of annoying to pay all that attention to my kids' activities!"***
>
> *Well, the process implemented by Vikido requires at least some initial parental intervention and consent. The parent needs to register the child, add and approve other family members, and the child can't login*

> *with its own password. We know... it ain't easy, but we did it anyway, because just like you, we rather spend a couple of minutes here and there, and make sure we don't put our kids in harm's way.*[12]

This is exactly the kind of innovation the FTC should be encouraging – with the full understanding that it may require modification down the road. Vikido's efforts here are working to achieve exactly the desired outcome from COPPA: Parental understanding, engagement and control. We ask that the FTC not only maintain the current models of parental consent, but also increase their availability. This way we can once again encourage and make economical the development of tools to help children.

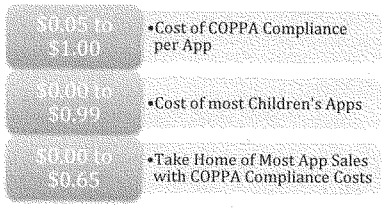
Challenges for App Developers

With every change, there are benefits and harms. We worry that in its effort to increase clarity, the FTC may have, inadvertently, created confusion for some app developers. This ranges from difficulties in app development and optimization to the inability to produce low cost, high quality apps for children.

Costs of Compliance with COPPA for App Developers - Too often it seems that websites and developers try to avoid catering to those under 13 in an attempt to avoid dealing with the difficulties in compliance with COPPA. The requirements for parental consent are difficult and costly. Joining a safe-harbor program accompanies financial outlays. In face, the Commission stated,

> [I]t is unclear whether the economic burden on small entities will be the same as or greater than the burden on other entities ... in order to comply with the rule's requirements, *website operators will require the professional skills of legal ... and technical ... personnel* ... and that approximately *80% of such operators would qualify as small entities* under the SBA's Small Business Size standards.[13]

As the number of children using computers, tablets and smart phones increases, so do the opportunities to use these devices as learning tools. But to do so, there must be an economically viable platform on which these tools can be built. Current costs of acquiring parental consent range



[12] *See* http://vikido.com

[14] http://www.cooley.com/files/84589_ALERT_COPPAcoversMobile.pdf

from $0.05 to $1.00 per app. Such a barrier is too high for many small businesses, like many members of Moms with Apps (an online community of family friendly developers), especially when most app developers net only $0.75 or less per app sold. Accordingly, we ask that the Commission simplify compliance with COPPA, and thus decrease the costs of compliance to these small entities.

Treatment of UDID as Personal Information – The addition of UDID to the list of personal information under COPPA creates unexpected consequences to app developers' ability to improve and develop their apps. For example, app developers often use a UDID for analytics purposes: seeing what parts of their apps kids like best or least, and using this information to improve the existing and future products. This information is used exclusively as a type of data-point. While we at ACT think this collection falls under the "internal operations" exception, enough uncertainty remains warranting further clarification.

We recognize that the FTC's proposed definition of "support for the internal operations of the website or online service" includes "user authentication, improving site navigation, maintaining user preferences, serving contextual advertisements, and protecting against fraud or theft." However, we are uncertain if the collection for purposes of analytics invokes notice and consent requirements. Often the third-party terms-of-use allow the third-party to collect and store the UDID. With so few options for third-party analytics, app developers are stuck between a non-negotiable terms of use and COPPA regulations, and as an NPRM analysis by Cooley, LLP points out:

> *The FTC mentions parenthetically one example of a mobile application and an advertising network that collects information from within the application. No mention is given as to whether both the mobile application and the advertisement need to be directed toward children or whether both might be operators simply because either the mobile application or the advertisement is directed toward children. If the latter, this raises questions regarding whether parties have an obligation to conduct due diligence on the activities of the other party and the effect, if any, of contractual prohibitions on targeting children*[14].

A possible solution to this dilemma would be to expand the definition of "support for the internal operations of the website or online service" to explicitly include the collection for purposes of analytics even if by third parties.

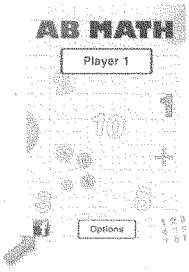
Treatment of User Name as Personal Information - A user name, like a UDID, without any other information is just a combination of letters. It does not necessarily identify any particular individual. Treating a user name as

[14] http://www.cooley.com/files/84589_ALERT_COPPAcoversMobile.pdf

personal information has unintended consequences for app developers. Because app developers also use user names to track popularity as opposed to UDIDs, the treatment of user name as personal information limits their ability to provide useful educational and fun services to children.

ACT spoke with educational developers who are members of Moms with Apps, an organization made up of more than 600 Moms (and now Dads) who create educational apps. Several developers we spoke with noted that educational apps need to enable parents and teachers to see if children did their reading, took the test, or completed the project made available through the app. As part of the process to enable this review, the app creates user names for the children. If user names are considered personal information it could chill such innovation.

Prompting the Sharing of PI is Collection - While it may seem obvious that the prompting or encouraging of a child to share personal information constitutes collection, the growth of social networking as a means to stay connected with kids and parents suggests a difference between "sharing" and "collecting." Our concern is that a developer adding a social networking button such as the Facebook "Like" button would automatically be in violation of COPPA, even though no direct information about the child is shared.



We do not believe that this is a scenario the FTC necessarily envisioned, but we ask that they review this outcome in the light of this limitation.

Prohibition on Advertising to Children - When COPPA was created, it was to protect children's privacy online, not to prevent marketing to children. In fact, legislators stated four different goals for COPPA[15] none of which included a probation of marketing to children. Moreover, advertising and interest-based advertising to children is not new. A child watching "Pokémon" will have likely seen an advertisement for Nintendo products since Nintendo knows that kids who like Pokémon may also like other Nintendo products. The company knows this since it is able to

[15] COPPA was created to "(1) to enhance parental involvement in a child's online activities in order to protect the privacy of children in the online environment; (2) to enhance parental involvement to help protect the safety of children in online form such as chatrooms, home pages, and pen-pal services in which children may make public postings of identifying information; (3) to maintain the security of personally identifiable information of children collected online; and (4) to protect children's privacy by limiting the collection of personal information from children without parental consent." 144 Cong. Rec. S11657 (daily ed. Oct. 7, 1998) (statement of Rep. Bryan).

collect information through services such as Neilson ratings that tracks the viewing habits of families, including their children.

App developers require the option to earn the nominal income generated from nominal advertising to children since app developers, especially those making apps for kids, charge little or no money for their products. Yet children desire creative, fun, and well-made apps. This prohibition would "raise costs for smaller or new sites and services geared toward minors"[16] and force app developers to choose between making lackluster and cheap apps, or utilize alternative revenue streams, like those from passive tracking, to create types apps kids want.

We worry that if the FTC enacts this complete prohibition, it will encourage app developers to drive to the bottom. Since most apps cost one dollar or less this means a drive to decrease quality. This is not something anyone wants.

Conclusion

The apps ecosystem is creating innovating new products for teachers, parents, and children. Moreover, it is creating jobs. As the FTC considers changes to COPPA outlined in the NPRM, we urge incredible attention to the potential risks that misstep could cost small businesses and stifle innovation. Nonetheless, the FTC has made great strides at updating COPPA. Faced with an evolving marketplace that provides innovative ways to make learning fun, the Commission has taken a measured approach to improve child safety. While it requires additional changes, we are not suggesting the FTC throw the NPRM out with the proverbial bath water.

We concur with the FTC's frequent reminder to Congress that the Commission possesses sufficient existing regulatory authority to address online child safety. The strength of the COPPA statute and the flexibility of the regulatory process provide effective means to update the Act without the need for additional legislation.

We thank you again for the opportunity to present testimony and we look forward to working you and the FTC in protecting children's privacy online and the innovators who are growing our economy.

[16] Written Testimony of Berin Szoka Senior Fellow, The Progress & Freedom Foundation & Director of PFF's Center for Internet Freedom, Hearing on "An Examination of Children's Privacy: New Technologies & the Children's Online Privacy Protection Act" April 29, 2010.

Mrs. BONO MACK. Thank you, Mr. Reed.

And just a side note, I appreciate the reference to California and the earthquake damage, though, up there on the wall is not my fault.

Mr. REED. You are bringing good apps, just not earthquakes.

Mrs. BONO MACK. Mr. Balkam, you are recognized for 5 minutes.

STATEMENT OF STEPHEN BALKAM

Mr. BALKAM. Thank you very much, Chairman and Ranking Member Butterfield and members of the subcommittee. My name is Stephen Balkam and I am the CEO of the Family Online Safety Institute. It gives me great pleasure to testify before you today at today's hearing.

We would like to applaud the chairman's leadership on these issues. The series of hearings held by this subcommittee are a prime example of an effective step that the government can take to balance the promotion of technological innovation with the need to keep children safe online.

FOSI is an international, non-profit membership organization working to make the online world a safer and healthier place for kids and their families, and we do this by identifying and promoting the best practice, tools, and methods in the field of online safety and privacy that also respect free speech. Personally, I have had over 16 years experience working in the Internet safety field and I am the proud father of two daughters. The views expressed in both my written and oral testimony are my own and do not necessarily reflect the views of all the FOSI members.

So the online landscape for all users has certainly changed in the past 11 years since COPPA was enacted, none more so than for children. We need a more sophisticated approach that empowers families to gain and maintain control of their digital lives. Simply put, in order to encourage safe and responsible online use, we need tools, rules, and schools: the technology tools of filters and monitoring devices; balanced laws, terms of use, and household rules; and education on good digital citizenship, online safety, privacy and security.

At FOSI, we believe in building a culture of responsibility to ensure that children have a safe and productive time on the Internet. We support balanced government oversight of industry self-regulatory efforts. This approach allows for maximum innovation and creative solutions, as well as the potential for enforcement actions and legislative intervention in the event of industry non-compliance.

Parental empowerment is an important component of this approach. Recent research commissioned by us and carried out by the Hart Research showed that 93 percent of parents have set rules or limits to monitor their children's online usage and 53 percent of parents have used parental controls. FOSI is working with industry to promote increased awareness of parental controls and education as to their use.

We commend Congress and the FTC for their work in providing reasonable government oversight through COPPA and its corresponding Rule, while encouraging self-regulation and promoting parental empowerment and children's responsibility. The FTC has

continued to evaluate the effectiveness of the Rule and propose revisions where necessary.

The planned revisions contain many positive aspects and ideas relating to the definition of a child, the actual knowledge standard, the expansion of parental consent requirements and methods, as well as proposed revisions to the safe harbor regime. We agree fully with the FTC's analysis that the current Rule is broad enough to encompass the technological advancements that have occurred in the past 11 years.

The COPPA statute defines child as "an individual under the age of 13," and we are pleased that the FTC has determined that it remains the appropriate age. Changes to the statutory definition could lead to a substantial increase in children lying about their age, or for that matter parents lying about their kids' age, and thus negate protections afforded to younger kids through COPPA and specific Web site protections for minors.

The FTC's enforcement mechanism foreseen in the original Rule has provided a flexible and valuable tool that has allowed the FTC to adapt to the changing technologies. Recent enforcement actions which we just heard about against W3 Innovations, an app developer, show that the FTC was able to use the Rule to ensure the compliance of a technology that was not widely available when COPPA was enacted.

The FTC's review of the Rule, in conjunction with their recent enforcement actions, demonstrates that no further action on the part of Congress is required at this time. The current system, with the FTC's proposed revisions, allows for privacy protection as well as technological innovations. Furthermore, attempts by Congress to pass legislation will almost certainly be rendered inadequate within a few years by the innovation of new methods of online interaction, sharing, and communication.

In my opinion, a positive step that Congress could take in this sphere would be to increase funding for Internet safety and privacy education in schools, as well as for research into children's online behaviors and attitudes. This would allow for all future legislative efforts to be founded on a factual basis.

Finally, I believe that the best way to ensure that children have productive, safe, and secure experiences on the Internet is through awareness, education, and empowerment. I would like to thank the subcommittee again for holding this timely and important hearing. We believe that with reasonable government oversight, the self-regulatory and multi-stakeholder approach currently being championed in the United States—although under attack in other parts of the world—can continue to protect kids and their privacy on the Internet without impeding technological innovation.

Thank you very much.

[The prepared statement of Mr. Balkam follows:]

Before the U.S. House of Representatives
Energy and Commerce Committee

Subcommittee on Commerce, Manufacturing and Trade

Hearing on "Protecting Children's Privacy in an Electronic World"

Statement of
Stephen Balkam, CEO, Family Online Safety Institute

October 5, 2011

Statement of Stephen Balkam
CEO, Family Online Safety Institute

Before the U.S. House of Representatives Energy and Commerce Committee
Subcommittee on Commerce, Manufacturing and Trade

Hearing on
"Protecting Children's Privacy in an Electronic World"

October 5, 2011

Chairman Bono-Mack, Ranking Member Butterfield, and Members of the Subcommittee, my name is Stephen Balkam and I am the CEO of the Family Online Safety Institute (FOSI). On behalf of FOSI, it gives me great pleasure to testify before you at today's hearing on "Protecting Children's Privacy in an Electronic World." We would like to applaud the Chairman's leadership on these issues. The series of hearings held by this Subcommittee are a prime example of an effective step that the government can take to balance the promotion of technological innovation with the need to keep children safe online.

FOSI is an international, non-profit membership organization working to make the online world a safer and healthier place for children and their families. We do this by identifying and promoting the best practices, tools and methods in the field of online safety and privacy that also respect free speech. FOSI's members represent the best of the Internet industry, including broadband providers, wireless carriers, social networking websites, technology companies, and major trade associations[1]. FOSI works as a trusted convener, bringing

[1] Members include: AOL, AT&T, BT Retail, Comcast, Disney, Entertainment Software Association, Facebook, France Telecom, Google, GSM Association, Microsoft, Motion Picture Association of America, NCTA,

together leaders in government, industry, and the nonprofit sectors to collaborate and innovate new solutions for online safety in a Web 2.0 world.

Personally, I have over 16 years' experience working in the Internet safety field. I gave testimony before the Senate Judiciary Committee on the Child Pornography Prevention Act of 1995[2] and I attended and spoke at the first White House Internet Summit in 1997[3]. I was appointed as a Commissioner of the Child Online Protection Act (COPA) Commission in 2000[4] and was a member of the Internet Safety Technical Task Force in 2008.[5] I worked closely with the National Cable and Telecommunications Association on the PointSmart-ClickSafe report in 2009.[6] The views expressed in both my written and oral testimony are my own and do not necessarily reflect the views of all the FOSI members.

On September 15, 2011[7] the Federal Trade Commission's (FTC) proposed changes to the Child Online Privacy Protection (COPPA) rule. The Act itself was passed in 1998 and became effective in 2000. The online landscape for all users has certainly changed in the past 11 years, none more so than for children. Gone are the days when we were primarily working to protect them from inappropriate material that they may come across online, now we are dealing with content that they themselves are producing, as well as troubling behaviors such as cyberbullying, sexting and online addiction. We need a more sophisticated approach that

---

Nominum, Optenet, RuleSpace, Sprint, StreamShield, Symantec, Time Warner Cable, Telefónica, USTelecom, The Wireless Foundation, Verizon and Yahoo!.

[2] *"Child Pornography Prevention Act of 1995"* United States Congress. Senate Committee on the Judiciary

[3] *"Internet Online Summit."* See http://www.kidsonline.org/participants/

[4] *"Commission on Online Child Protection."* See http://www.copacommission.org/report/

[5] *"Enhancing Child Safety & Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States."* See http://cyber.law.harvard.edu/pubrelease/isttf/

[6] *"Point Smart Click Safe: Task Force Recommendations For Best Practices For Child Online Safety."* See http://www.pointsmartreport.org/

[7] *"FTC Seeks Comment on Proposed Revisions to Children's Online Privacy Protection Rule"* See http://ftc.gov/opa/2011/09/coppa.shtm

empowers families to gain and maintain control of their digital lives. Simply put, in order to encourage safe and responsible online use we need tools, rules and schools: the tech tools of filters and monitoring devices; balanced laws, terms of use and household rules; and education on good digital citizenship, online safety, privacy and security.

Building a Culture of Responsibility Online

At FOSI we believe in building a culture of responsibility to ensure that children have a safe and productive time on the Internet. In order to foster good digital citizenship, six different areas of society need to work together. These are:

1) Reasonable government oversight and support;

2) Fully resourced law enforcement;

3) Robust and comprehensive industry self-regulation;

4) Tech-savvy teachers;

5) Empowered parents; and

6) Resilient children making wise choices about the content they access and post online, the people they contact, the people they allow to contact them and how they conduct themselves online.

We support balanced government oversight of industry self-regulatory efforts. This approach allows for maximum innovation and creative solutions as well as the potential for enforcement actions and legislative intervention in the event of industry non-compliance. As part of this, we promote robust and comprehensive industry self-regulation in this space. As a membership organization we bring together the leading technology companies to discuss emerging issues and create best practices and new solutions to increase privacy measures for children and adults alike.

We need more tech-savvy teachers to help foster 21st Century skills including digital and media literacy, and good cyber-ethics. By teaching children to make wise choices on the Internet, they can protect themselves and their peers from some of the risks that exist online. The skills that they learn will continue to assist them throughout their digital lives.

Parental empowerment is an important component of this approach. Recent research commissioned by FOSI and carried out by Hart Research Associates[8] showed that 96% of parents questioned say that they have spoken to their children about their online behavior, 87% report awareness of Internet parental controls available and 53% of parents have used them. Among those parents who do not use parental controls 60% state that the reason that they don't is because they have household rules and limits in place. FOSI is working with industry to promote increased awareness of parental controls and education as to their use, and believes that these efforts are key to help parents make informed decisions about the sites their children access online and the information that they share.

In accordance with this multi-stakeholder approach, FOSI commends Congress and the FTC for their work in providing reasonable government oversight through the Children's Online Privacy Protection Act and its corresponding Rule, while encouraging self-regulation and promoting parental empowerment and children's responsibility.

Proposed Revisions to Children's Online Privacy Protection Rule

[8] "*Who Needs Parental Controls? A Survey Of Awareness, Attitudes, And Use Of Online Parental Controls.*" http://www.fosi.org/research.html

Since it became effective in 2000 the FTC has conducted two reviews of the Rule,[9] a roundtable discussion with representation from industry, non-profit and government,[10] as well as commencing a number of enforcement actions against those found to be in contravention of the Rule[11].

The FTC continues to evaluate the effectiveness of the Rule and propose revisions where necessary. The most recent report was released on September 15, 2011[12] and the comment period for the notice of proposed rulemaking is open until November 28, 2011. This provides an opportunity for those impacted by the Rule, as well as all stakeholders to provide input into the proposals before the new provisions come into force.

The planned revisions contain many positive aspects and ideas relating to the definition of a child, the actual knowledge standard, the expansion of parental consent requirements and methods as well as proposed revisions to the safe harbor regime. We agree fully with the FTC's analysis that the current Rule is broad enough to encompass the technological advancements that have occurred in the past 11 years.

The COPPA statute, and thus the Rule, define child as "an individual under the age of 13,"[13] the FTC had asked for comments on whether or not the age should be increased or altered.

---

[9] *"Children's Online Privacy Protection Rule: Request for Comments."* April 21, 2010 http://www.ftc.gov/os/2005/04/050420coppacomments.pdf *"FTC Seeks Comment on Proposed Revisions to Children's Online Privacy Protection Rule"* September 16, 2011 See http://ftc.gov/opa/2011/09/coppa.shtm

[10] *"Protecting Kids' Privacy Online. Reviewing the COPPA Rule"* June 2, 2010 Roundtable. See http://www.ftc.gov/bcp/workshops/coppa/index.shtml

[11] *"Operators of Online "Virtual Worlds" to Pay $3 Million to Settle FTC Charges That They Illegally Collected and Disclosed Children's Personal Information"* May 12, 2011 See http://www.ftc.gov/opa/2011/05/playdom.shtm and *"Mobile Apps Developer Settles FTC Charges It Violated Children's Privacy Rule"* August 15, 2011 See http://www.ftc.gov/opa/2011/08/w3mobileapps.shtm

[12] *"FTC Seeks Comment on Proposed Revisions to Children's Online Privacy Protection Rule"* See http://ftc.gov/opa/2011/09/coppa.shtm

[13] s.1302 Children's Online Privacy Protection Act 1998

FOSI is pleased to see that the FTC has determined that 13 remains the appropriate age.[14] EU research released this year found that there were increasing numbers of children under 13 accessing social networks, against their terms of use.[15] Changes to the statutory definition could lead to a substantial increase in children lying about their age, and thus negate protections afforded to younger children through COPPA and specific website protections for minors.

FOSI commends the FTC on maintaining the 'actual knowledge' standard, rather than substituting the 'constructive knowledge' alternative.[16] We believe that such a requirement would be wholly unworkable and would impose unmanageable burdens on all website operators.

FOSI supports the Commission's decision to look for additional methods to obtain verifiable parental consent.[17] The newly proposed system will allow for innovation and flexibility in the future. Concerns have been expressed about some of the proposed techniques, including the use of parents' government IDs and video-conferencing, but we are hopeful that the FTC will conduct full risk-assessments and will not maintain data for longer than is necessary, as well as considering the burden that can be imposed on small businesses through the use of suggested methods.

In accordance with the emphasis attributed to parental empowerment in FOSI's online culture of responsibility, we are pleased to see the introduction of 'just-in-time' notifications for

[14] II. COPPA's Definition of "Child" Federal Register. Vol. 76, No. 187
[15] *"Social Networking, Age and Privacy"* Livingstone, S., Ólafsson, K.& Staksrud, E. 2011
[16] III. COPPA's "Actual Knowledge" Standard Federal Register Vol. 76, No. 187
[17] "(1) Mechanisms for Verifiable Parental Consent" Federal Register Vol. 76, No. 187

parents and the simplification of privacy policies.[18] In order that the consent is full and informed, it is vital that parents understand what their children are doing online and what they are consenting to. The encouragement of industry and websites to improve transparency is welcomed. The FTC's increased oversight of the safe harbor programs, with the periodic reporting of COPPA compliance that proposed in the revisions,[19] is a positive step to ensure increased transparency and accountability.

The FTC's enforcement mechanism foreseen in the original Rule has provided a flexible and valuable tool that has allowed the FTC to adapt to the changing technologies. Recent enforcement actions against W3 Innovations LLC, an app developer[20], show that the FTC was able to use the Rule to ensure the compliance of a technology that was not widely available when COPPA was enacted. Other enforcement actions, such as that against Playdom, Inc[21], demonstrate that the FTC is able to obtain consent decrees that have both a restitution element as well as imposing increased reporting, by the wrongdoer, of COPPA compliance.

The FTC's review of the Rule, in conjunction with their recent enforcement actions, demonstrates that no further action on the part of Congress is required at this time. The current system, with the FTC's proposed revisions, allows for privacy protection as well as technological innovation.

---

[18] "(2) Direct Notice to a Parent" Federal Register Vol. 76, No. 187
[19] "F. Safe Harbors" Federal Register Vol. 76, No. 187
[20] *"Mobile Apps Developer Settles FTC Charges It Violated Children's Privacy Rule"* August 15, 2011 See http://www.ftc.gov/opa/2011/08/w3mobileapps.shtm
[21] *"Operators of Online "Virtual Worlds" to Pay $3 Million to Settle FTC Charges That They Illegally Collected and Disclosed Children's Personal Information"* May 12, 2011 See http://www.ftc.gov/opa/2011/05/playdom.shtm

Government Actions

At FOSI we advocate reasonable government supervision with informed lawmaking based on a foundation of robust research. We also encourage restraint in areas we feel that industry is being pro-active and is offering effective solutions to child protection and privacy. It is with this in mind that we express caution in respect to H.R. 1895, the "Do Not Track Kids Act of 2011"[22], as well as international proposals from the European Commission and the International Telecommunications Union.

The Supreme Court, in a number of decisions,[23] has found that children under 18 are entitled to some, if more limited, first amendment protections. It is our concern that the "Do Not Track Kids Act of 2011" though laudable in its aims would be unconstitutional and technologically impracticable. The concept of the 'eraser button' presents legal, technical and practical issues. Firstly, it would conflict with journalistic autonomy and press freedoms, in allowing requests for stories about those under 18 to be arbitrarily removed from the Internet. Furthermore, there is no real explanation for how such a 'button' would be developed technically, while the practical issues that come with such an idea, such as the verification of an individual's identity prior to a deletion request and the issues that shared content present, make it almost totally infeasible. Additionally, we believe that with the proposed revisions to the COPPA Rule many of the provisions within H.R. 1895 become arguable unnecessary and adequate protection is given to children's privacy.

[22] H.R. 1895, the "Do Not Track Kids Act of 2011"
[23] *Tinker v. Des Moines Independent Community School District*, 393 U.S. 503 (1969) and *Board of Education v. Pico*, 457 U.S. 853 (1982)

There is increased concern about national governments of other countries, as well as international bodies overreaching, with a potentially global effect. While we applaud the balance of regulation, oversight and self-regulatory efforts which are embodied in COPPA, we are mindful of proposed legislation from international bodies such as the European Union[24] and the International Telecommunication Union (ITU)[25]. Both recommend the imposition of a top-down approach that requires industry-wide, rather than technology specific, actions. The plans carry with them the threat of legislation if the European Commission or ITU feel that the mandated self-regulatory approach is not working. Any laws or initiatives enacted by these bodies would require strict compliance by US technology companies operating within these jurisdictions.

For more information on these and many other international initiatives, you can refer to www.fosigrid.org, an online portal which aggregates online safety initiatives, legislation and education efforts from over 100 countries around the world, as well as all fifty U.S. states.

At FOSI, we caution the government not to overreach. Currently the FTC is doing a consummate job in proposing new provisions in response to the changing nature of the technology, as well as working to educate parents on protecting their children's privacy. Moreover, the 2011 revisions work to increase transparency and improve upon the existing safe harbor scheme.

In our opinion a positive step that Congress could take in this sphere would be to increase funding for Internet safety and privacy education in schools as well as for research into

[24] "*Digital Agenda: further action needed to safeguard children – Commission report*" September 13, 2011 See http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/1026

[25] Internet Telecommunication Union "*Child Online Protection Global Initiative.*" See http://www.itu.int/osg/csd/cybersecurity/gca/cop/

children's online behaviors and attitudes. A good example of such a proposal is S. 1047 the School and Family Education about the Internet (SAFE Internet) Act[26] introduced by Senator Menendez in 2009. The legislation foresaw a system of grants to carry out Internet safety education programs and research, to be administered by the Secretary of Education and the Secretary of Health and Human Services. This would allow for all future legislative efforts to be founded on a factual base.

Conclusion

In summary, we at FOSI do not believe that there is a need for further governmental action at this time. The admirable work of the FTC in reviewing the COPPA Rule, using the existing mechanisms to keep up with technological innovation and enforcing the Rule against those in breach render them the best suited organization to ensure that children remain safe and private online. The speed at which the technology has developed over the last decade means that any attempt by Congress to pass legislation will almost certainly be rendered inadequate within a few years by the innovation of new methods of online interaction, sharing and communication.

It should be noted, however, that the best way to ensure that children have productive, safe and secure experiences on the Internet, with all the opportunities that it brings, is through awareness, education and empowerment.

FOSI would like to thank the Subcommittee again for holding this timely and important hearing. We believe that with reasonable government oversight, the self-regulatory and multi-

[26] S. 1047 the School and Family Education about the Internet (SAFE Internet) Act. See http://thomas.loc.gov/cgi-bin/query/z?c111:S.1047:#

stakeholder approach currently being championed in the United States can continue to protect children and their privacy on the Internet without impeding technology innovation. FOSI looks forward to working with Members of the Subcommittee as they pursue these issues further. Thank you again for the opportunity to testify today, and I welcome your questions.

Mrs. BONO MACK. Thank you.
Dr. Montgomery, you are recognized for 5 minutes.

STATEMENT OF KATHRYN C. MONTGOMERY

Ms. MONTGOMERY. Thank you very much, Chairman Bono Mack, Ranking Member Butterfield, and the other members of the subcommittee. I really appreciate the opportunity to be here to talk about children's privacy. It was during the 1990s in the mid-1990s that I started investigating what was going on with online children's Web sites, and I was very disturbed to find that because of the increasing value of children as a target market and their avid involvement with the Internet, companies were setting up Web sites all over the web that had a business model really based on taking a lot of personal information from children and offering prizes and doing all kinds of things in order to get children to give up personal information. One of my favorites was the Batman site that said "be a good citizen of Gotham and fill out the census." And there were many, many others like that.

And I did not hear when I went to industry meetings and when I read all the cited coverage about all this any mention of children's privacy, any concerns raised in the industry, and that is why we went to the FTC. I was pleased that I was able to work with both sides of the aisle in Congress, with the FTC, with the Coalition of Child Health, and consumer groups, and with industry stakeholders to craft a statute and a set of regulations that would successfully balance our collective interests in nurturing the growth of commerce on the Internet while protecting the privacy of our children.

And because decades of research had already identified that younger children had particular vulnerabilities to advertising, one of the key goals of the law was to prevent online companies from targeting individual children with marketing messages. COPPA has served, as many people have observed here, as an effective safeguard for young consumers under the age of 13, and it sent a strong signal to the industry if you are going to do business with our Nation's children, you will have to follow some rules. And that was built into the system. As a result, some of the most egregious data collection practices that would have become state-of-the-art were curtailed.

Today, however, children are growing up in a ubiquitous 24/7 digital media environment. The data collection practices that we identified in the '90s have been eclipsed by a new generation of tracking and targeting techniques. The Commission's proposed rules for updated COPPA offer a careful, well-researched, and sensible set of recommendations for addressing many of these practices, and I want to briefly highlight three of them.

The first, which others have mentioned is mobile and other location devices. Roughly half of all children have mobile phones now by the age of 11. You can ask any parent. Advertising is growing on mobile technologies. Geolocation makes it possible to target kids wherever they are. This raises not only marketing abuse issues and privacy issues but also safety issues. I think the agency has appropriately clarified that COPPA should apply to mobile and other web-connected location devices.

The second issue concerns this notion of what is personally identifiable information. I was a participant in the 2010 June roundtable at the FTC. I was quite taken with the amount of consensus among a wide spectrum of participants that these days there is really no longer a meaningful distinction between personal information and such "non-personal information" as persistent cookies and IP addresses. And the Wall Street Journal did an investigation last year showing that a lot of these things are being placed routinely on children's sites.

While the FTC proposed rules would then apply COPPA safeguards to protect children from companies that want to use the tools to behaviorally target individual children or to create profiles or share the information, the rules are also narrowly tailored so that they wouldn't interfere with what the companies are doing in terms of their regular normal business operations. And I think this kind of sensitivity is reflective of how the FTC has done a good job here.

By the way, on mobile phones, I am disappointed about text messaging. I hope we can talk about that because we know how much kids are using texts.

And finally, I agree with the Commission that the mechanism of parental verification that we created with COPPA is not appropriate for teens. However, I do feel strongly that adolescents can no longer be ignored in the public policy debates over online privacy. We know they are being encouraged to share a lot of information. They also do not know how all of their data are tracked by all of these other kinds of technologies that are now online. I hope the FTC will develop some specific recommendations in its broader privacy agenda.

And the goal of any public policy on teen privacy should balance the ability of young people to participate fully in the digital media culture with the government and industry's obligation to ensure that youth are not subjected to unfair deceptive surveillance, data collection, or behavioral profiling. The legislation offered by Representative Joe Barton and Representative Ed Markey known as the Do Not Track Kids Act of 2011 is based on these principles and it is to give teens themselves the power to make their own decisions about their privacy online. If we can build privacy principles into how our online businesses engage with both children and adolescents, we can help ensure that young people are treated fairly in the digital marketplace and that they grow up with an understanding of their rights and responsibilities as consumers.

Thank you.

[The prepared statement of Ms. Montgomery follows:]

Summary of Testimony
Kathryn C. Montgomery, PhD
House Subcommittee on Commerce, Manufacturing, and Trade
Hearing: Protecting Children's Privacy in an Electronic World
October 5, 2011

Congress enacted the Children's Online Privacy Protection Act (COPPA) with strong bi-partisan support. For more than a decade, COPPA has served as an effective safeguard for young consumers under the age of 13 in the online marketing environment. Because the legislation was passed during the early stages of Internet e-commerce, COPPA established a clear set of "rules of the road" to help guide the development of the children's digital marketplace. As a result, some of the most egregious data collection practices that were becoming state of the art in the online marketing environment were curtailed. Though the law took effect in the formative period of Internet marketing, it was purposely designed to adapt to changes in both technology and business practices, with periodic reviews by the FTC to ensure its continued effectiveness. Today's children are growing up in a ubiquitous digital media environment, where mobile devices, instant messaging, social networks, virtual reality, avatars, interactive games, and online video have become ingrained in their personal and social experience. Members of this generation of young people are, in many ways, living their lives online. With the current expansion of digital media platforms and the growing sophistication of online data collection and profiling, however, it is now critically important that the intent of COPPA be fully implemented to protect young people from new commercial practices in today's digital media environment.

The Federal Trade Commission has taken a responsible, inclusive, and thoughtful approach to its current review of the COPPA rules, enlisting the input of a wide range of experts and stakeholders in a series of workshops, discussions, and written comments over the past several years. The proposed rules announced last month offer a careful, well-researched, reasoned, and sensible set of recommendations, reflecting the interests and concerns of the many participants involved in the Commission's widespread consultation efforts. We believe the changes suggested by the FTC will help address a number of problems raised by consumer groups, privacy experts, and child advocates. The FTC's proposed safeguards on location and mobile information are especially timely, given the dramatic increase in children's use of these devices.

Finally, while COPPA has established an important framework for safeguarding our youngest consumers in the digital marketplace, adolescents have no such protections. The goal of any public policy on teen privacy should be to balance the ability of young people to participate fully in the digital media culture—as producers, consumers, and citizens—with the governmental and industry obligation to ensure that youth are not subjected to unfair and deceptive surveillance, data collection, or behavioral profiling. The legislation offered by Rep. Joe Barton and Rep. Edward Markey, known as the "Do Not Track Kids Act of 2011," is based on these principles.

BEFORE THE
The Subcommittee on Commerce, Manufacturing, and Trade
of the
House Committee on Energy and Commerce

Hearing: Protecting Children's Privacy in an Electronic World

October 5, 2011

TESTIMONY OF
Kathryn C. Montgomery, PhD
Professor, School of Communication
American University, Washington, DC

Chairman Bono Mack, Ranking Member Butterfield, and members of the subcommittee. I appreciate the opportunity to testify before you today about children's privacy in the digital world, and the important role of the Children's Online Privacy Protection Act (COPPA). During the 1990's, while president of the nonprofit Center for Media Education (CME), I played a leadership role in the passage of COPPA, working with a coalition of prominent education, health, and consumer groups.

As you know, Congress enacted COPPA in 1998 with strong bi-partisan support, led by Senator John McCain (R-Ariz.), Representative Edward Markey (D-Mass), and then-Senator Richard Bryan of Nevada. My colleagues and I worked closely with these congressional leaders and with other members, as well as with the Federal Trade Commission, on the legislation. We also consulted with a broad spectrum of stakeholders, including online industry groups, to craft a statute and a set of regulations that would successfully balance our collective interests in nurturing the growth of commerce on the Internet, while protecting the privacy of our children.

For more than a decade, COPPA has served as an effective safeguard for young consumers under the age of 13 in the online marketing environment. Because the legislation was passed during the early stages of Internet e-commerce, COPPA established a clear set of "rules of the road" to help guide the development of the children's digital marketplace. As a result, some of the most egregious data collection practices that were becoming state of the art in the online marketing environment were curtailed.[1] Though the law took effect in the formative period of Internet marketing, it was purposely designed to adapt to changes in both technology and business practices, with periodic reviews by the FTC to ensure its continued effectiveness. With the current expansion of digital media platforms and the growing sophistication of online data collection and profiling, however, it is now critically important that the intent of COPPA be fully implemented to protect young people from new commercial practices in today's digital media environment.

As I document in my book, *Generation Digital: Politics, Commerce and Childhood in the Age of the Internet,* the emergence of the World Wide Web ushered in a host of online marketing and data collection practices that raised fundamental privacy concerns for children. The business model of one-to-one marketing, combined with the increasing value of children as a target market for advertisers, created a perfect storm for companies that wanted to use the Internet to take advantage of young people. Numerous commercial websites offered prizes and other incentives to encourage children to supply personal information about themselves. For example, one site targeted at "young investors," urged children to provide an astonishing amount of financial information, including any gifts they might have received in the form of stocks, cash, savings bonds, mutual funds or certificates of deposit. Another site, set up to promote the movie *Batman,* encouraged children to "be good citizens of Gotham" and fill out the "census."[2] Some of these practices were so disturbing that the Center for Media Education enlisted the help of Georgetown University Law Center's Institute for Public Representation to file a complaint with the FTC in 1996. The commission found our complaint persuasive and, with the urging of our coalition and others, began examining the commercial children's online data collection market.[3] The FTC's internal research

played a key role in documenting the rampant spread of data collection and the failure of self-regulatory promises by industry. The commission's report, released just months prior to passage of COPPA, provided crucial evidence of the need for this important law.[4]

Congress made a wise decision in 1998 to enact COPPA. I believe the law has been a clear legislative success. It was a balanced and sensible solution to a challenging problem. It established a level playing field by creating a law that applied to every commercial player—from the largest children's media companies to the smallest start-ups. And it sent a strong signal to the growing online marketing industry: If you are going to do business with our nation's children, you will have to follow some basic rules. Because decades of research documented younger children's particular vulnerabilities to advertising and marketing, one of the key goals of the law was to prevent online companies from targeting individual children with marketing messages.[5] COPPA was narrowly tailored to apply only to commercial websites that were directed at children under the age of 13, or where there was actual knowledge by the website operator that the user was under that age. Marketers were prevented from using under-the-radar techniques to solicit information from children, without notifying and seeking permission from parents in advance. In keeping with fair information principles, COPPA was also intended to minimize the collection of personally identifiable data from children, and to eliminate the practice of offering prizes and other incentives to encourage such data collection. All of these measures have helped create a safer and more responsible online environment for children.[6]

No law is perfect, as everyone in this body is well aware. In the case of COPPA, children who are under 13 can lie about their age when visiting sites that are not intended for them. And not all parents are willing or able to be involved in the day-to-day online navigations of their children. But COPPA has helped to ensure that online marketers build privacy into the design of their children's services, requiring them to abide by a social compact for treating their youngest consumers with fairness and sensitivity. By establishing a safe harbor provision, COPPA created a system whereby self-regulatory guidelines—developed and implemented by a

number of private groups—operate within a framework of clear government rules and enforcement authority by the FTC. Industry organizations, such as the Council of Better Business Bureau's Children's Advertising Review Unit (CARU), for example, have incorporated children's online privacy guidelines into their codes of conduct to ensure that children's media and marketing companies fully understand their obligations under the law, and to provide ongoing monitoring of industry practices, referring companies that do not abide by the rules to the FTC.[7] We are also pleased that the Commission has taken the initiative to examine and respond to specific cases, cracking down on those practices that violated the statute.[8]

Recent developments in the online marketing arena, however, pose new challenges that warrant the attention of both the FTC and Congress. The Web has matured, thanks especially to broadband and mobile technologies. As a result, not only has the digital marketplace grown dramatically, but it has also become an even stronger presence in the lives of young people. Today's children are growing up in a ubiquitous digital media environment, where mobile devices, instant messaging, social networks, virtual reality, avatars, interactive games, and online video have become ingrained in their personal and social experience. Members of this generation of young people are, in many ways, living their lives online.

As *Advertising Age* reported last year, children aged 2 to 11 had the biggest increase among any age group using the Internet online in the period 2004 to 2009. The same report explains that according to a Nielsen Online survey conducted in July 2009, "Time spent online for children ages 2 to 11 increased from about 7 hours to more than 11 hours per week, or a jump of 63% over five years."[9] Children are especially adept at simultaneously engaging with multiple platforms. A 2011 study of 6-12 year olds found that approximately "36% of kids go online while watching live TV and 30% are visiting social networks."[10] By 2015, some 25.7 million children will be online.[11] As of the first quarter of 2011, the children's online market comprised more than 20 million 2-11 year olds, according to comScore, with children frequenting numerous child-oriented websites, including Nick.com, Miniclip, Poptropica, Webkinz, Disney, and Barbie.com.[12]

Children continue to be a highly valuable target market for advertisers, with ad time on TV and new media platforms generating record sales.[13] Market researchers note that young people between the ages of 8 and 15 "control $43 billion in spending annually." Advertisers know as well that children influence the purchasing decisions of their parents, "from small ticket items like soft drinks to major family purchases such as automobiles."[14] They are also using new media technologies at an earlier age, one of many trends closely monitored by the online marketing industry.[15] As *eMarketer* noted in June 2011, commenting on the "Always Connected" report by the Joan Ganz Cooney Center at Sesame Workshop, "[T]he amount of time kids between 4 and 8 spend online increases significantly as they age. More than 80% of children ages 4 to 5 consume digital media, and more than 90% of those ages 6 to 8 do so."[16] The Cooney report, noted a recent story in *Adweek,* "found that 80 percent of kids under the age of 5 use the Internet weekly, and 60% of kids 3 and younger are now watching videos online."[17] Some 10 percent of 6-8 years olds, 23 percent of 9-10 year olds, and 41 percent of children aged 11-12 are social network users, according to eMarketer.[18]

Mobile phone use has risen dramatically among children. As a 2010 study by the Kaiser Family Foundation noted, "Over the past five years, there has been a huge increase in [cell phone] ownership among 8- to 18-year-olds: from 39% to 66%.... During this period, cell phones... have become true multi-media devices: in fact, young people now spend more time listening to music, playing games, and watching TV on their cell phones (a total of :49 daily) than they spend talking on them (:33)."[19] Today, by age 11, "half of kids have cellphones," according to research released this year by LMX Family/Ipsos OTX. That same report, explained *Advertising Age,* noted that "pre-schoolers [are] adopting digital habits or being exposed to new devices even faster than tweens, a sign of the speed with which digital technology is reshaping media and marketing habits for the youngest children."[20] The mobile phone is "the ultimate ad vehicle," commented one media executive, "the first one ever in the history of the planet that people go to bed with."[21] Children 6-12 use their cell phones to surf the Internet, download applications, update their social networks and also, as we know, send and receive

text messages.[22] Last April, Nielsen reported that "Children begin downloading apps on a parents' phone at an average age of 9 years old," and parents explained that "30 percent of the apps on their phones were installed by their kids."[23] Children of color are particularly avid users of mobile and other new technologies.[24]As the "Always Connected" study explained, when African-American and Hispanic children own mobile phones, they "spend more time talking, texting and using media on cell phones than white children." Lower-income Black and Hispanic children, it notes, "consume more digital media overall than their higher-income white peers." [25]

Unlike television, where children's exposure to commercials is limited to relatively brief intervals during the times when they are viewing the programs, the ubiquity of the digital media culture means that marketing is now woven into the very fabric of young people's daily experiences, following them wherever they go on a 24/7 basis. As a consequence, children are increasingly exposed to a flood of digital marketing and data collection techniques, many of which operate below the level of parental or public awareness. Today's contemporary practices are increasingly multidimensional—simultaneously and purposefully integrated into Facebook, Twitter, YouTube, and other social media, in order to encourage interactive, word-of-mouth, and user-generated marketing. The growth of online video, interactive games, and virtual worlds, coupled with the increasingly immersive nature of all digital media, mean that young people are not just *viewing content,* but *inhabiting media environments* where entertainment, communication, and marketing are combined in a seamless stream of compelling sounds and images. The impact of marketing is further enhanced and intensified by new forms of monitoring and measurement that were not possible before the advent of digital media. Increasingly, these various types of analysis can take place in real time, following users' movements and behaviors from moment to moment, and assessing their reactions to various advertising and sales appeals. As a result, marketing messages can be tested, refined, and tailored for maximum effect.[26]

The online data collection practices we originally identified in the 1990s have been eclipsed by a new generation of tracking and targeting techniques, as online data collection has entered a new era.[27] Growing investments in online marketing

and data collection companies are expanding the field's capacity to deliver advertising based on the harvesting of an individual users' online data.[28] An entire infrastructure of companies has emerged, specializing in data collection and sales, including demand-side platforms, data exchanges, and data-optimization services. Vast amounts of user data are now regularly mined and stored in behavioral targeting warehouses and other databases—and used in an instant to update online targeting profiles. "Data has become one of the most valuable commodities in the real-time bidding system," explained a recent industry report.[29]

Behavioral targeting uses a range of online methods—including cookies and other invisible data files—to learn about the unique interests and online behaviors through the tracking and profiling of individual users. Through web analytics, conversation targeting, and other forms of surveillance, marketers can now track individuals online, across media, and in the real world, monitoring their interactions, social relationships, and locations. As noted on September 27, 2011, by Rep. Joe Barton and Rep. Ed Markey in their letter to the FTC asking for an investigation of so-called "supercookies," and as reported by the *Wall Street Journal*, "companies have been installing supercookies on users' computers without their knowledge." An example of the growing data collection arsenal, supercookies "allow websites to collect detailed personal data about users, including websites previously visited. Even when consumers choose to delete regular cookies from their computers, supercookies persist."[30]

Recent advances in behavioral targeting are enabling marketers to more accurately predict and influence user behavior. For example, "predictive behavioral targeting" combines data from a number of different sources and makes inferences about how users are likely to behave in their response to marketing messages.[31] So-called "smart" ads stealthily learn about the behavior and interests of individual users and can have offers personalized in nearly real time based on data collection.[32] Increasingly, behavioral profiles incorporate information from outside databases.[33] Social media platforms are engaged in an expanding array of data collection practices that are unknown to most of their users. For example, social media marketing companies routinely track and analyze the flow of comments among

friends, in order to identify and potentially target the most "influential" person of the group.[34] New forms of so-called "real-time buying" on advertising exchanges enable a consumer—even young ones—to be tracked, profiled, and sold to the highest bidder in milliseconds. [35]

Mobile marketing—combining text messaging, mobile video, and other new applications—is one of the fastest growing digital commerce platforms throughout the world, and a particularly effective way to reach and engage children.[36] Mobile devices are nearly ubiquitous; smart phones enable access to a rich array of Internet applications, including those taking advantage of GPS; local advertisers have new, inexpensive tools to deliver ads on mobile phones and in stores; and social networks are expanding their enterprises into the mobile arena, through ventures such as FourSquare, Gowalla, and Facebook's own location-based services.[37] Mobile marketers have incorporated behavioral targeting along with location information into their targeting practices.[38] Advertising on mobile devices is likely to become especially powerful, since it can target users by combining both behavioral and location data.[39] Ads on mobile phones will be able to reach young consumers when they are near a particular business and offer electronic pitches and discount coupons.[40] These new mobile marketing techniques also raise serious safety issues. As the coalition of children's, privacy, and consumer groups noted in their comments to the FTC, "Geolocation's threat to privacy extends beyond advertising. Information collected through geolocation is especially sensitive given that it can allow for a child to be physically contacted wherever he or she is, at any time. Even more concerning, a child's location information can be collected automatically, so neither the parent nor the child knows about, much less consents to, such collection."[41]

While current COPPA rules are able to provide safeguards against some of these emerging practices, developments are happening so quickly in the digital marketing industry that many of the new techniques may be escaping scrutiny by policy makers and industry self-regulatory bodies. Last year, the *Wall Street Journal* conducted an investigation of 50 websites popular with U.S. children and teens, discovering that more than 4,000 "cookies," "beacons," and other pieces of tracking

technology were placed on the computers of those who visited the sites. "Marketers are spying more on young Internet users than on their parents, building detailed profiles of their activities and interests," the *Journal* found. Eight of the websites in the survey were owned by Viacom's Nickelodeon, and an average of 81 tracking tools were installed on the computers that accessed those sites.[42]

Congress intended COPPA's basic framework to be flexible, anticipating the continued growth of digital media, and requiring the FTC to update its rules in order to ensure that the law's implementation would cover new ways of collecting personal information from children.[43] The Commission has taken a responsible, inclusive, and thoughtful approach to its current review of the COPPA rules, enlisting the input of a wide range of experts and stakeholders in a series of workshops, discussions, and written comments over the past several years. The proposed rules announced last month offer a careful, well-researched, reasoned, and sensible set of recommendations, reflecting the interests and concerns of the many participants involved in the Commission's widespread consultation efforts. We believe the changes suggested by the FTC will help address a number of problems raised by consumer groups, privacy experts, and child advocates.[44] The proposals have already garnered bi-partisan support, as well as praise from leading consumer and child advocacy groups.[45]

I would like to highlight several issues that I see as especially important. COPPA's flexible language was designed to ensure it would cover emerging technology and software applications as the digital landscape continued to grow. I am part of a broad coalition of consumer, children, and privacy groups that has urged the FTC to clarify that its rules encompass the full range of Internet-enabled or -connected services, including the increasingly ever-present cell phones children use, along with Web-connected gaming devices and online, interactive video.[46] I am pleased that the Commission has included these clarifications in its proposed rules.[47] The FTC's proposed safeguards on location and mobile information are especially timely, given the dramatic increase in children's use of these devices. These changes will help provide safeguards to address a number of new and emerging data collection techniques, such as "geo-fencing," which enables mobile

marketers to create a "pre-defined, virtual space around a particular location" and know when a child is "is within a determined radius."[48] I was disappointed that the proposed rules do not cover text messaging through SMS services on mobile phones, especially since texting is a particularly popular pastime for children, as well as a tool that digital marketers have seized upon to target young people. I understand the jurisdictional issues identified by the Commission, and I urge policy makers to find ways for ensuring children's privacy is adequately protected on mobile phones.

The second point I want to make concerns the issue of what constitutes personally identifiable information (PII). Since the 90s, when I first began my work on children's privacy, the techniques used to track, profile, identify, target, and retarget individuals in the digital environment have become highly sophisticated. As a consequence, the distinctions between personal and so-called non-personal information are quickly disappearing. This is particularly the case with the proliferation of personal digital devices such as smart phones and Internet-enabled gaming consoles, which are increasingly associated with individual users, rather than families.[49] As a participant in the FTC's June 2010 roundtable session on this issue, I was struck by the strong consensus among experts from industry, education, and the consumer community that there is no longer a meaningful distinction between such "non-personal" information as cookies, IP addresses, Web beacons, and the like, and the collection of one's actual email address and name. This means that marketers do not need to know the name, address, or email of a user in order to identify and target that particular individual.[50] While recognizing the technological changes and prevailing business practices that have eroded anonymity on the Internet, the Commission has proposed a very narrow and careful policy for bringing COPPA rules up to date. The proposal would enable online companies to use IP addresses and other persistent identifiers in order to conduct normal business operations (including serving contextual advertisements to children), but would create safeguards when the information was used to behaviorally target an individual child, create a profile based on that child's online activities, or share the information with third parties.[51]

The safe harbor programs established by COPPA play an essential role in the implementation of the law, establishing a workable system of self-regulation, enabling the creation of industry standards and practices, ensuring widespread adoption of the rules, and providing government oversight. However, there is a need for stronger accountability in order to ensure that these self-regulatory regimes serve their intended purpose. We agree with the Commission's call for greater rigor in the administration of these programs, including a requirement that they conduct annual reviews of how their member organizations are implementing children's privacy rules in their own business practices.[52]

Finally, while COPPA has established an important framework for safeguarding our youngest consumers in the digital marketplace, adolescents have no such protections. Today's teens are being socialized into this new digital culture, which resonates so strongly with many of their fundamental developmental tasks, such as identity exploration, social interaction, and autonomy.[53] Unlike any previous mass medium, the Internet makes it possible for young people to search for information on their own, taking advantage of online search tools to seek help for their personal problems, find support groups for handling emotional crises in their lives, and sometimes to talk about things they do not feel comfortable or safe discussing with their own parents.[54] Teenagers are particularly enthusiastic participants in social media platforms, which provide a user-friendly template for exploring their identities, sharing their favorite photos, music, and videos, and interacting with their friends.[55] But as young people integrate these new tools into their personal and social lives, they remain largely unaware of the subtle, often covert ways that digital media make it possible for companies to track, profile, and target them.

I agree with the Commission that the mechanism of parental verification established by COPPA to protect children under 13 is not appropriate for teens. However, I feel strongly that adolescents can no longer be ignored in the public policy debates over online privacy. The leading self-regulatory organizations have incorporated the children's privacy provisions into their codes of conduct. But none of them has acknowledged any special responsibilities to adolescents.[56] Child

advocacy and health groups have urged the FTC to develop specific recommendations for protecting the privacy of adolescents as part of its broad new initiative on online privacy.[57]

Some people have argued that teens are already savvy about online commercial practices, and thus need no protections.[58] However, a growing body of research within the fields of neuroscience, psychology, and marketing has identified key biological and psychosocial attributes of the adolescent experience that may make members of this age group particularly susceptible to many of the interactive marketing and data collection techniques that are increasingly pervasive in digital media.[59] Moreover, the data collection system that underlies so much online marketing is not transparent. Young people are being continually urged to make more of their personal information available in real time, including their location, yet research indicates the few consumers—including adults—really comprehend how that information is collected and used.[60] The prevailing practice of posting privacy policies on company websites is based on the assumption that consumers will read the policies, and if they do not like the terms, will "opt out." But most privacy policies offer no real choice; instead, the policies are presented as a "take-it-or-leave-it" proposition. Surveys have shown that most adults don't read, nor can they readily understand, the often confusing, technical legalese that characterizes these policies.[61] For under-aged youth, these challenges are further complicated. As the children's coalition explained in comments to the FTC, "...teenagers, who have less education and are less likely to make the effort to read privacy policies," are "more willing to forgo learning about or protecting against behavioral advertising practices... in order to more quickly and freely access websites and socially interact."[62]

Even when social networks provide mechanisms for setting one's individual privacy preferences, such settings may create a false sense of security for members, who are not aware of the myriad ways that marketers can still follow their behaviors, compile detailed profiles, and engage in behavioral targeting. The recent controversy over Facebook's decision to begin tracking users' actions even after they had logged off the site is an illustration of how default data collection practices

are often not visible to the public. As privacy advocates noted in a letter to the FTC this past week, "These changes in business practices give the company far greater ability to disclose the personal information of its users to its business partners than in the past. Options for users to preserve the privacy standards they have established have become confusing, impractical, and unfair."[63]

Without question, digital media play a critically important role in the positive development of young people.[64] The goal of any public policy on teen privacy should be to balance the ability of young people to participate fully in the digital media culture—as producers, consumers, and citizens—with the governmental and industry obligation to ensure that youth are not subjected to unfair and deceptive surveillance, data collection, or behavioral profiling. Policies should also be designed to ensure that young people are socialized to be responsible consumers in the growing digital marketplace, and to understand their rights. The onus of responsibility should not be placed on youth alone to protect themselves, but also on the companies that market to them.

The legislation offered by Rep. Joe Barton and Rep. Edward Markey, known at the "Do Not Track Kids Act of 2011," is based on these principles.[65] Under this bipartisan privacy bill, online companies targeting adolescents would have to "bake-in" reasonable "privacy by design" and age-appropriate safeguards that embody Fair Information Practices Principles. Unlike COPPA, no parental permission would be required when collecting personal information from adolescents; instead, teens themselves would be empowered to make their own decisions about their privacy online. I believe that the bill's common sense approach is something that all of us—parents, child advocates, online companies, and policymakers alike—would support.

Since the 1990s, Congress has played a key role in establishing privacy protections for young people in the online environment. I urge the committee to continue its proactive leadership on this important issue.

---

[1] A study in the *Journal of Consumer Affairs* found that more than 95 percent of the top 100 children's websites in the United States post privacy policies complying with COPPA's

requirements for information collection and use. Andrea J. S. Stanaland, May O. Lwin, and Susanna Leong, "Providing Parents with Online Privacy Information: Approaches in the US and the UK," *Journal of Consumer Affairs* 42 n. 3 (Fall 2009): 474, 484-85; See also Anthony D. Miyazaki, Andrea J. S. Stanaland, and May O. Lwin, "Self-Regulatory Safeguards and the Online Privacy of Preteen Children, *Journal of Advertising* 38, n. 4 (Winter 2009): 79, 83.

[2] Kathryn Montgomery, *Generation Digital: Politics, Commerce, and Childhood in the Age of the Internet* (Cambridge, MA: MIT Press, 2007); For a full discussion of COPPA's history, see Chapter 4, pp. 67-106; Kathryn Montgomery and Shelly Pasnik, *Web of Deception: Threats to Children from Online Marketing* (Washington, DC: Center for Media Education, 1996).

[3] Federal Trade Commission, "FTC Staff to Survey Consumer Privacy on the Internet,"26 Feb. 1998, http://www.ftc.gov/opa/1998/02/webcom2.shtm; Federal Trade Commission, "Privacy Online: Fair Information Practices in the Electronic Marketplace," May 2000, www.ftc.gov/reports/privacy2000/privacy2000text.pdf (both viewed 26 Apr. 2010).

[4] Federal Trade Commission, "Privacy Online: A Report to Congress," June 1998, http://www.ftc.gov/reports/privacy3/priv-23a.pdf (viewed 26 Apr. 2010).

[5] Dale Kunkel, "The Role of Research in the Regulation of U.S. Children's Television Advertising," *Knowledge: Creation, Diffusion, Utilization* 12, no. 1 (1990): 101-119. See also Deborah Roedder John, Consumer Socialization of Children: A Retrospective Look at Twenty-Five Years of Research," *Journal of Consumer Research* 26 (1999): 183-213.

[6] The FTC's COPPA rule applies to "Operators of commercial web sites and online services directed to children under 13 that collect personal information from them; operators of general audience sites that knowingly collect personal information from children under 13; and operators of general audience sites that have a separate children's area and that collect personal information from children under 13." Children's Online Privacy Protection Act, Federal Trade Commission. http://www.ftc.gov/privacy/privacyinitiatives/childrens.html (viewed 26 Apr. 2010).

[7] Children's Advertising Review Unit, "About the Children's Advertising Review Unit (CARU)," http://www.caru.org/about/index.aspx (viewed 26 Feb. 2011).

[8] See, for example, Federal Trade Commission, "Iconix Brand Group Settles Charges Its Apparel Web Sites Violated Children's Online Privacy Protection Act," 20 Oct. 2009, http://www.ftc.gov/opa/2009/10/iconix.shtm (viewed 26 Apr. 2010).

[9] Beth Snyder Bulik, "The On-Demand Generation," *Advertising Age* Insights White Paper, 12 Apr. 2010, http://adage.com/whitepapers/whitepaper?id=17 (purchase required).

[10] Wendy Goldman Getzler, "Co-entertainment, Media Multitasking on the Rise," Kidscreen, 13 Apr. 2011, http://kidscreen.com/2011/04/13/co-entertainment-media-multitasking-on-the-rise/#ixzz1ZRwoGWQd. Another study released last year found that "Small children today are more likely to navigate with a mouse, play a computer game and increasingly—operate a smartphone—than swim, tie their shoelaces or make their own breakfast." AVG, "Forget Swimming and Riding a Bike—Young Children Today More Likely to Have Mastered Computer Games: AVG Study Shows Young Kids Learn Tech Skills Before Life Skills," 19 Jan. 2010, http://www.avg.com/us-en/press-releases-news.ndi-672 (both viewed 2 Oct. 2011).

[11] Jared Jenks, "Demographic Profile—Children," eMarketer, Feb. 2011, http://www.emarketer.com/Report.aspx?code=emarketer_2000736 (Purchase required).

[12] comScore, "Entertainment-Kids, Q1, 2011," personal copy. For additional information on comScore's analysis of the online children's market, see "An Upcoming Change to comScore US Weighting," comSAcore U.S. Client Newsletter, Aug. 2011, http://www.comscore.com/newsletter/2011/August/US_Client_Newsletter#story4 (viewed 2 Oct. 2011).

[13] Anthony Crupi, "Upfront: The Kids Are All Right: Younger Set's Bizarre Expected to Top $1 Billion," *Adweek*, 28 Mar. 2011, http://www.adweek.com/news/advertising-branding/upfront-kids-are-all-right-126382 (viewed 2 Oct. 2011).

[14] Demographic Profile-Children. eMarketer; http://www.millwardbrown.com/Solutions/AreasOfExpertise/KidsTweensTeens.aspx

[15] "A child's first cell phone, first game system and his or her exposure to technology are all happening earlier," according to Donna Sabino, senior vice president of Kids and Family Insights at Ipsos OTX Media CT. Quoted in Getzler, "Co-entertainment, Media Multitasking on the Rise."

[16] "Young Children Consuming More Digital Media," eMarketer, 9 June 2011, http://www.emarketer.com/Articles/Print.aspx?1008435 (viewed 2 Oct. 2011).

[17] Brian Braiker, "The Next Great American Consumer: Infants to 3-year-olds: They're a New Demographic Marketers are Hell-bent on Reaching," *Adweek*, 26 Sept. 2011, http://www.adweek.com/news/advertising-branding/next-great-american-consumer-135207 (viewed 2 Oct. 2011).

[18] "US Child Social Network Users, by Age," eMarketer, Feb 2011, personal copy.

[19] Kaiser Family Foundation, "Daily Media Use Among Children and Teens Up Dramatically from Five Years Ago," 20 Jan. 2010, http://www.kff.org/entmedia/entmedia012010nr.cfm (viewed 7 Apr. 2010).

[20] "Of households with preschoolers, 38% had handheld gaming devices vs. only 24% among those with children aged 6-12. Preschool households also held an edge in laptops (82% to 76%), gaming consoles (76% to 63%) and internet-capable cellphones (69% to 65%)." Jack Neff, "CyberTots: Pre-teens Drive iPad Purchases, Join Social Networks," *Advertising Age*, 20 Apr. 2011, http://adage.com/article/news/pre-teens-drive-ipad-purchases-join-social-networks/227101/ (viewed 2 Oct. 2011).

[21] Abbey Klaassen, "Why Google Sees Cellphones as the 'Ultimate Ad Vehicle,'" *Advertising Age*, 8 Sept. 2008, http://adage.com/mobilemarketingguide08/article?article_id=130697 (viewed 4 Aug. 2009).

[22] "Mobile Phone Activities of US Children, 2009 & 2011," eMarketer, 10 May 2011, personal copy.

[23] "U.S. Parents Say Almost A Third of the Apps on Their Phone Were Downloaded by Their Children," Nielsen Wire, 27 Apr. 2011, http://blog.nielsen.com/nielsenwire/online_mobile/u-s-parents-say-almost-a-third-of-the-apps-on-their-phone-were-downloaded-their-children/ (viewed 2 Oct. 2011).

[24] See, for example, examples of targeting Hispanic, African-American and Asian-American youth at Interactive Food & Beverage Marketing: Targeting Children & Youth in the Digital Age," http://digitalads.org/findrecords.php (viewed 2 Oct. 2011).

[25] Aviva Lucas Gutnick, Michael Robb, Lori Takeuchi, and Jennifer Kotler, "Always Connected: The New Digital Media Habits of Young Children," The Joan Ganz Cooney Center at Sesame Workshop, 2011, p29. For general background on multicultural digital targeting, see, for example, Cheryl Pearson-McNeil and Todd Hale, "Dissecting Diversity: Understanding the Ethnic Consumer," Nielsen Wire, 19 May 2011, http://blog.nielsen.com/nielsenwire/consumer/dissecting-diversity-understanding-the-ethnic-consumer/print/; Google/GlobalHue/Ipsos OTX MediaCT, U.S., "Five Truths of the Digital African American Consumer: A Digital Culture of Change," June 2011, http://www.gstatic.com/ads/research/en/2011_Five_Truths_Digital_African_American_Consumer.pdf; Google/OTX, U.S., "US Hispanic Auto Consumers," Mar. 2011, http://www.gstatic.com/ads/research/en/2011_US_Hispanic_Auto.pdf (all viewed 2 Oct. 2011).

[26] See Kathryn Montgomery, Sonya Grier, Jeff Chester, and Lori Dorfman, "Food Marketing in the Digital Age: A Conceptual Framework and Agenda for Research," Apr. 2011, http://digitalads.org/reports.php (viewed 2 Oct. 2011).

[27] For a detailed description of the latest trends in online behavioral profiling and data collection, see "Comments of the Center for Digital Democracy, et al, In the Matter of A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: Proposed Framework for Business and Policymakers," 18 Feb. 2011, http://www.democraticmedia.org/files/2011-02-18-teen-privacy.pdf (viewed 2 Oct. 2011).

[28] See, for example, Devindra Hardawar, "Google Acquires Invite Media to Help Users with Ad Exchanges," VentureBeat, 2 June 2010, http://venturebeat.com/2010/06/02/google-acquires-invite-media-to-help-users-with-ad-exchanges/; David Kaplan, "VC Money Keeps Pouring In For Ad Targeters: Turn Raises $20 Million," paidContent.org, 5 Jan. 2011, http://paidcontent.org/article/419-vc-money-keeps-pouring-in-for-ad-targeters-turn-raises-20-million/ (both viewed 15 Feb. 2011).

[29] Econsultancy, "Demand-Side Platforms Buyer's Guide," 2011, p. 3, http://econsultancy.com/us/reports/dsps-buyers-guide (purchase required).

[30] "Barton, Markey Urge FTC To Investigate Use of 'Supercookies,'" 27 Sept. 2011, http://markey.house.gov/index.php?option=com_content&task=view&id=4527&Itemid=141 (viewed 2 Oct. 2011).

[31] See for example, "Predictive Behavioral Targeting Firm Launched, Gets Big VC Backing," *Online Media Daily*, 9 June 2011, http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=152060 (viewed 2 Oct. 2011).

[32] See, for example, Yahoo, "Smart Ads," http://advertising.yahoo.com/article/smart-ads.html. Google's Teracent also provides such ads. Teracent, "Advertiser Solutions," http://www.teracent.com/advertiser-solutions/ (both viewed 2 Oct. 2011).

[33] Experian, "Digital Advertising," http://www.experian.com/business-services/digital-advertising.html; TargusInfo, "Our Solutions: On-Demand Verification," http://www.targusinfo.com/solutions/verification/ (both viewed 2 Oct. 2011).

[34] See, for example, "Clearspring Announces Audience Delivery Of 200mm US Uniques Across Top Dsps and Exchanges," 25 Apr. 2011, http://www.clearspring.com/about/press/clearspring-launches-audiences-everywhere; Teresa Basich, "Social Media Measurement & Analysis," 1 Mar. 2010, http://www.radian6.com/blog/2010/03/social-media-measurement-analysis/; Sysomos, "Social Media Monitoring Tools for Business," http://www.sysomos.com/ (all viewed 2 Oct. 2011).

[35] See, generally, AdExchanger.com, http://www.adexchanger.com/; ExchangerWire.com, http://www.exchangewire.com/ (both viewed 2 Oct. 2011); Econsultancy, "Online Advertising Survey," Sept. 2011, http://econsultancy.com/us/reports/online-advertising-survey (purchase required).

[36] Enid Burns, "U.S. Mobile Ad Revenue to Grow Significantly through 2013," ClickZ, 25 Feb. 2009, http://www.clickz.com/3632919 (viewed 4 Aug. 2009).

[37] John Bell, "Brands: Claim Your Facebook Place Today," The Digital Influence Mapping Project, 23 Aug. 2010, http://johnbell.typepad.com/weblog/2010/08/brands-claim-your-facebook-place-today.html (viewed 31 Dec. 2010).

[38] See Greg Dowling, "Mobile Measurement," presentation at Engage 2011, Dan Francisco, 28 Feb - 3 Mar. 2011, http://engage.webtrends.com/blog/category/media-type/presentation/ (viewed 2 Oct. 2011); Dai Pham, "Smartphone User Study Shows Mobile Movement Under Way," Google Mobile Ads Blog, 26 Apr. 2011, http://googlemobileads.blogspot.com/2011/04/smartphone-user-study-shows-mobile.html (viewed 2 Oct. 2011); eMarketer, "Leading Mobile Ad Targeting Tactics According to Advertisers/Agencies in North America," Aug. 2011, personal copy; Marc Theermann, "Making Mobile RTB Smarter," Admeld Blog, 7 Sept. 2011, http://www.admeld.com/blog/view/Making-Mobile-RTB-Smarter/ (viewed 2 Oct. 2011).

[39] Center for Digital Democracy and U.S. PIRG, "Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Mobile Marketing Practices," Federal Trade Commission Filing, 13 Jan. 2009, http://www.democraticmedia.org/current_projects/privacy/analysis/mobile_marketing (viewed 7 June 2009).

[40] A. Johannes, "McDonald's Serves Up Mobile Coupons in California," *PROMO Magazine*, 26 Oct. 2005, http://promomagazine.com/incentives/mcds_coupons_102605/ (viewed 4 Aug. 2009).

[41] Institute for Public Representation (on behalf of the Center for Digital Democracy, American Academy of Child and Adolescent Psychiatry, the American Academy of Pediatrics, Benton Foundation, Berkeley Media Studies Group, Campaign for a Commercial Free Childhood, Center for Science in the Public Interest, Children Now, Consumer Action, Consumer Federation of America, Consumer Watchdog, Consumers Union, National Consumers League, Privacy Rights Clearinghouse, Public Health Institute, U.S. PIRG, and World Privacy Forum), filing with the Federal Trade Commission "In the Matter of Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule," 30 June 2010, http://www.ntia.doc.gov/legacy/comments/101214614-0614-01/attachments/COPPA_Final.pdf (viewed 2 Oct. 2011).

[42] Steve Stecklow, "On the Web, Children Face Intensive Tracking," *Wall Street Journal*, 17 Sept. 2010, http://online.wsj.com/article/SB10001424052748703904304575497903523187146.html ; Robert D. Hof, "Ad Networks Are Transforming Online Advertising," *BusinessWeek*, 19 Feb. 2009, http://www.businessweek.com/magazine/content/09_09/b4121048726676.htm (both viewed 2 Oct. 2011).

[43] See, especially, Section 1302980(F) of COPPA.

[44] Federal Trade Commission, "FTC Seeks Comment on Proposed Revisions to Children's Online Privacy Protection Rule," 15 Sept. 2011, http://www.ftc.gov/opa/2011/09/coppa.shtm (viewed 2 Oct. 2011).

[45] "Markey, Barton Praise FTC's Proposed Updates to COPPA Rule," 15 Sept. 2011, http://markey.house.gov/index.php?option=com_content&task=view&id=4509&Itemid=141; "Consumers Union Praises FTC Proposal to Improve, Update Rules for Children's Online Privacy," 16 Sept. 2011, http://news.consumerreports.org/baby/2011/09/consumers-union-praises-ftc-proposal-to-improve-update-rules-for-childrens-online-privacy.html (both viewed 2 Oct. 2011).

[46] Federal Trade Commission, "FTC to Host Public Roundtable to Review Whether Technology Changes Warrant Changes to the Children's Online Privacy Protection Rule," 19 Apr. 2010, http://www.ftc.gov/opa/2010/04/coppa.shtm; Federal Trade Commission, "FTC Seeks Public Comment on Program to Keep Web Site Operators in Compliance With the Children's Online Privacy Protection Rule," 6 Jan. 2010, http://www.ftc.gov/opa/2010/01/isafe.shtm (both viewed 26 Apr. 2010).

[47] Federal Trade Commission, "FTC Seeks Comment on Proposed Revisions to Children's Online Privacy Protection Rule."

[48]Placecast, "Shopalerts," http://placecast.net/shopalerts/index.html; Placecast, "PlaceAd," http://placecast.net/placead/index.html; Navteq media Solutions, "LocationPoint Advertising," http://navteqmedia.com/mobile/advertising/locationpoint-advertising (all viewed 2 Oct. 2011).

[49] Federal Trade Commission, "FTC Seeks Comment on Proposed Revisions to Children's Online Privacy Protection Rule." See also Common Sense Media, "Do Smart Phones = Smart Kids?" 21 Apr. 2010, http://www.commonsensemedia.org/about-us/news/press-releases/do-smart-phones-smart-kids (viewed 2 Oct. 2011).

[50] Federal Trade Commission, "Protecting Kids' Privacy Online: Reviewing the COPPA Rule," 2 June 2010, http://www.ftc.gov/bcp/workshops/coppa/index.shtml (viewed 12 Sept. 2011). Federal Trade Commission (Bureau of Consumer Protection), "A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, 1 Dec. 2010, pp. 35-38, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf (viewed 23 Feb. 2011). The European Union has also weighed in on this issue, supporting the concept that behavioral targeting information is tied to individuals. Data Protection Working Party, "Opinion 2/2010 on Online Behavioural Advertising, 22 June 2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf (all viewed 13 Sept. 2011). See also Wendy Davis, "ClearSight Launches Targeting Platform Tying IP Addresses To Offline Data," *Online Media Daily*, 28 June 2010,

http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=131044 (viewed 2 Oct. 2011).

[51] Federal Trade Commission, "FTC Seeks Comment on Proposed Revisions to Children's Online Privacy Protection Rule."

[52] Federal Trade Commission, "FTC Seeks Comment on Proposed Revisions to Children's Online Privacy Protection Rule."

[53] S. Harter, "Processes Underlying the Construction, Maintenance and Enhancement of the Self-concept in Children," *Psychological Perspective on the Self* 3 (1990): 45-78; U. Uhlendorff, "The Concept of Developmental Tasks," *Social Work & Society* 2, n. 1 (2004): 54-63; J. Hill, "Early Adolescence: A Framework," *Journal of Early Adolescence* 3, n. 1 (1983): 1-21; K. Subrahmanyam and P. Greenfield, "Online Communication and Adolescent Relationships," *The Future of Children* 18, n. 1 (2008): 119-146.

[54] Montgomery, *Generation Digital: Politics, Commerce, and Childhood in the Age of the Internet,* 141-177; Subrahmanyam and Greenfield, "Online Communication and Adolescent Relationships."

[55] H. Marcus and P. Nurius, "Possible Selves," *American Psychologist* 41, n. 9 (1986): 954-969. S. Stern, "Producing Sites: Exploring Identities: Youth Online Authorship," in D. Buckingham, ed. *Youth, Identity, and Digital Media*, pp. 99-117.

[56] Network advertising Initiative, "The NAI Releases the Updated 2008 NAI Principles," http://www.networkadvertising.org/networks/principles_comments.asp; Children's Advertising Review Unit, "CARU Privacy Program," http://www.caru.org/program/index.aspx; Children's Advertising Review Unit, "Supporters," http://www.caru.org/support/supporters.aspx; "Self-Regulatory Principles of Online Behavioral Advertising," Implementation Guide, Oct. 2010, http://www.aboutads.info/principles (all viewed 2 Oct. 2011).

[57] Center for Digital Democracy, "Consumer, Privacy, Child Health & Advocacy Groups Comments on FTC's Proposed Privacy Framework—Protection for Teens," 18 Feb. 2011, http://www.centerfordigitaldemocracy.org/consumer-privacy-child-health-advocacy-groups-comments-ftcs-proposed-privacy-framework-protection-te (viewed 3 Oct. 2011).

[58]Alice E. Marwick, Diego Murgia Diaz, and John Palfrey, March 2010, "Youth, Privacy, and Reputation: Literature Review," p. 10, http://cyber.law.harvard.edu/publications/2010/Youth_Privacy_Reputation_Lit_Review (viewed 2 Oct. 2011).

[59] C. Pechmann, L. Levine, S. Loughlin, *et al.*, "Impulsive and Self-conscious: Adolescents' Vulnerability to Advertising and Promotion," *Journal of Public Policy & Marketing* 24, n. 2 (2005): 202-221. Frances M. Leslie, Linda J. Levine, Sandra E. Loughlin, and Cornelia Pechmann, "Adolescents' Psychological & Neurobiological Development: Implications for Digital Marketing," http://digitalads.org/reports.php (viewed 2 Oct. 2011); S. Livingstone and E. J. Helsper, "Does Advertising Literacy Mediate the Effects of Advertising on Children? A Critical Examination of Two Linked Research Literatures in Relation to Obesity and Food Choice," *Journal of Communication* 56, n. 3 (2006): 560-584. A. Nairn and C. Fine, "Who's Messing with My Mind? The Implications of Dual-process Models for the Ethics of Advertising to Children," *International Journal of Advertising* 27, n. 3 (2008): 447-470.

[60] Joseph Turow, "Americans and Online Privacy: The System is Broken," A Report from the Annenberg Public Policy Center of the University of Pennsylvania, June 2003, http://www.asc.upenn.edu/usr/jturow/internet-privacy-report/36-page-turow-version-9.pdf (viewed 23 Feb. 2011).

[61] Institute for Public Representation (on behalf of the American Academy of Child and Adolescent Psychiatry, et al), filing with the Federal Trade Commission concerning "Online Behavioral Advertising Principles."

[62] Institute for Public Representation (on behalf of the American Academy of Child and Adolescent Psychiatry, et al), filing with the Federal Trade Commission concerning "Online Behavioral Advertising Principles." pp. 9, 7.

[63] Letter to Jon Leibowitz, Chairman, Federal Trade Commission from Marc Rotenberg, Executive Director, Electronic Privacy Information Center, September 28, 2011.

[64] MIT Press, "The John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning," http://mitpress.mit.edu/catalog/browse/browse.asp?btype=6&serid=170; John D. and Catherine T. MacArthur Foundation, "Building the Field of Digital Media and Learning," http://digitallearning.macfound.org/site/c.enJLKQNlFiG/b.2029199/k.94AC/Latest_News.htm; Kathryn Montgomery, Barbara Gottlieb-Robles, and Gary O. Larson, "Youth as E-Citizens: Engaging the Digital Generation" (Washington, DC: American University, 2004), http://www.centerforsocialmedia.org/ecitizens/index2.htm (all viewed 26 Apr. 2010).

[65] "H.R. 1895: Do Not Track Kids Act of 2011," http://www.govtrack.us/congress/bill.xpd?bill=h112-1895&tab=summary (viewed 2 Oct. 2011).

Mrs. BONO MACK. Thank you.
Mr. Simpson, you are recognized for 5 minutes.

STATEMENT OF ALAN SIMPSON

Mr. SIMPSON. Good morning, Ms. Bono Mack, Ranking Member Butterfield, and thank you to all the members of the subcommittee for this important hearing. I am Alan Simpson. I am with Common Sense Media, and I want to begin by outlining that Common Sense Media works as a nonprofit, nonpartisan organization dedicated to helping children and families thrive in a world of media and technology. One way that we describe our work is that we love media. We work with everyone to make it better for kids. We admire and embrace many of the innovations we have seen in this space in recent years, and we believe that parents, educators, companies, and policymakers all must play a central role in helping to protect children's privacy in this rapidly changing electronic world. And we work with each of these groups to improve the media lives and the privacy opportunities of children.

The Federal Trade Commission's proposed rule revisions will help keep COPPA up to date with this rapidly changing world. They will improve protections for children's online privacy, encourage parental involvement, and foster innovation in online services for children, especially the innovations we most need—innovations to protect children. The COPPA recommendations will help hold the industry more accountable, and most importantly, they will build on the fundamental purpose of COPPA, which is bolstering the role of parents as the informed gatekeepers in the lives of their young children. This is not a question of whether kids will be online or offline. We all know that kids are online and they will always be online. It is most a question of who will be watching them and who will be watching over them when they are online.

I would like to echo Dr. Montgomery's remarks about the value of the FTC recommendations and emphasize most of all that the FTC has struck a careful and reasonable balance between maintaining the internal operations of online services and protecting children from intensive tracking and behavioral advertising.

The FTC proposals will be important steps for younger kids, but teens still need protections and they need empowerment, and the legislation Mr. Barton mentioned—H.R. 1895—will be a strong baseline for those protections and that empowerment.

In my written remarks, I have outlined in more detail the work that Common Sense Media is doing with parents and schools, including dozens of articles that we have published in the last year and a half around privacy and security. And many of those parent tips that we published are among the most popular resources on our site for parents.

We also work in more than 18,000 schools around the country providing the education around smart, responsible use of media and privacy and security are an essential part of that. But one of the most important parts of this equation are the media and technology companies themselves, and we feel they must do far more to help parents and families protect children's online privacy in part because they are in the best position to develop better technology, better tools, and better information for users. There have

been positive steps in this area of late, but on the whole, media and technology companies have not done enough to provide better solutions for families. Parents need the innovators to innovate to protect. In our experience, the companies will, especially if they are encouraged by this subcommittee and this Congress to do so.

Thank you.

[The prepared statement of Mr. Simpson follows:]

Prepared Statement of:

Alan Simpson

Vice President of Policy

Common Sense Media

United States House of Representatives

Energy and Commerce Committee

Subcommittee on Commerce, Manufacturing and Trade hearing:

Protecting Children's Privacy in an Electronic World

October 5, 2011

Summary of Prepared Statement of Alan Simpson, Common Sense Media

- This hearing is critical, because concerns about children's online privacy are growing.
- Common Sense Media believes that parents, educators, companies, and policymakers all must play a central role in helping to protect children's privacy in an electronic world. We work with each of these groups to improve the media lives of children.
- The Federal Trade Commission's proposed rule revisions will help keep COPPA up to date with a rapidly changing electronic world. They will improve protections for children's online privacy, encourage parental involvement, and foster innovation in online services for children. They will help hold industry more accountable. The revisions also build on the fundamental purpose of COPPA – bolstering the role of parents as informed gatekeepers in the lives of their young children.
- It is especially valuable that the FTC has clarified that COPPA covers mobile platforms, and has struck a reasonable balance between maintaining the internal operations of online services and protecting children from intensive tracking and behavioral advertising.
- The FTC proposals will be an important step for younger kids, but teens still need protection, and legislation has been introduced that would provide a strong baseline.
- Media and technology companies must do far more to help families protect children's online privacy, because they are in the best position to develop better technology, tools and information for users. There have been a few positive steps by industry of late, but on the whole, media and technology companies have not done nearly enough to provide better solutions for families. In general, they only respond to government pressure.

Good morning, Madam Chairwoman and members of the Subcommittee, and thank you for this opportunity to discuss continuing updates for the protection of children's privacy. Today we address the Federal Trade Commission's proposed rule revisions for the Children's Online Privacy Protection Act (COPPA) and the need for further policy action to empower parents and protect children's privacy.

Common Sense Media is a non-profit, non-partisan organization dedicated to helping children and families thrive in a world of media and technology. We do this by providing trustworthy information, education, and an independent voice, and by working with everyone involved in the growing role of media in the lives of kids – parents and families, educators, media and technology companies, and policymakers.

Families and children are obviously the first and most important audience, and the major focus of our work. More than one and a half million people visit the Common Sense website each month for reviews about media content (including movies, video games, mobile applications or "apps," web sites, and books) and parent tips about the digital media world.

In addition, we have built an extensive and free Digital Literacy and Citizenship curriculum and parent education program for schools and educators.[1] These research-based tools provide lesson plans, classroom and homework activities, and interactive components that help teachers and parents guide students from K-12 to make smart, safe and responsible decisions in the digital world where they live, study and play. We launched the curriculum two years ago, and there are now more than 18,500 schools using the resources, in all 50 states.[2]

Media and technology companies are also an essential part of the equation, and our distribution partnerships with leading companies like Comcast, DIRECTV, Time Warner

[1] http://www.commonsensemedia.org/educators
[2] For example: CA – 1874 schools; NC – 517; TN – 281; FL – 696; AR – 130; IL – 759; KS – 230; KY – 233; LA – 182; MI – 503; MS – 96; NY – 1106; NH – 150; NJ – 505; TX – 1137; WV – 66; UT – 94

Cable, Cox Communications, Yahoo!, Google, AOL, Apple, Disney, Netflix, and Fandango enable tens of millions of parents to access our advice and information.

In addition, policymakers play a key role in helping families and kids thrive in a world of media and technology, and the current discussions about children's online privacy are a great example. Common Sense Media commends the Chair and the Subcommittee for this timely hearing on children's privacy. The FTC's proposed revisions will help keep COPPA up to date with a rapidly changing and increasingly mobile electronic world. They will significantly improve protections for children's online privacy, encourage parental involvement, and foster innovation in online services for children. Most importantly, the revisions build on the fundamental purpose of COPPA – maintaining the role of parents as gatekeepers in the lives of their children. As Senator Bryan stated when introducing the Senate version of COPPA:

> Senator McCain and I believe there must be safeguards against the online collecting of information from children without a parent's knowledge or consent. If a child answers a phone and starts answering questions, a parent automatically becomes suspicious and asks who they are talking to. When a child is on the Internet, parents often have no knowledge of [with] whom their child is interacting.[3]

While the FTC revisions will keep COPPA's protections for children under 13 up to date, there are still important online privacy concerns for adolescents aged 13 and older. We look forward to further action from the Commission on protections for adolescents in their Privacy Framework, and we look forward to further Congressional action in this area. There are several sensible proposals for strengthening protections for privacy and personal information online. Because of our focus on children and families, Common Sense Media is

[3] 144 Cong. Rec. S8483 (July 17, 1998) (Statement of Sen. Bryan).

especially supportive of H.R. 1895, the "Do Not Track Kids Act of 2011" proposed by Rep. Edward Markey (D-Mass.) and Rep. Joe Barton (R-Texas).

I. The Time Is Critical

Revisions to the COPPA rule are clearly needed now, because the electronic world has changed dramatically since the law was written in 1998 – and the changes are even more significant for kids. Children and teens today are growing up in an electronic environment that provides an ever-present and ever-changing experience – an environment that is changing childhood itself. And kids don't just access content online, they create it. They don't simply interact online with their peers, but with adults and companies too. In contrast to the childhoods many of us had, today's children are growing up in public. They post, search, copy, friend, tweet, check in, create, distribute, and connect through social networks, apps, and other services in ways that can be seen by millions, and tracked by companies, around the world.

Concern about online privacy is clearly growing. In a Common Sense Media/Zogby International poll last fall, 85% of parents said they are more concerned about online privacy than they were five years ago. 61% of parents said Congress should update laws related to online privacy and security for children and teens.[4]

Those survey findings are reinforced by growing demand for Common Sense parent tips and educator resources. In the past year we have published more than two dozen parent advice articles, curriculum lessons, and videos related to online privacy and security. These pages have been viewed more than 100,000 times on our site, and the curriculum documents have been downloaded by more than 3,000 teachers.

[4] Common Sense Media, *Protecting Our Kids' Privacy in a Digital World*, 1 (Dec. 2010). http://cdn2-www.ec.commonsensemedia.org/sites/default/files/privacy_whitepaper_dec2010.pdf.

Data from our media and technology company partners provide another illustration about parent concerns around online privacy and safety for children:

- Each month, more than 800,000 people visit the Yahoo! Safely site to access parent information – from Common Sense and other organizations – on issues like cyberbullying, privacy protection, and digital citizenship.
- Through partnerships with Comcast, Time Warner Cable, DIRECTV, Bright House, Cox, and others, Common Sense provides video-on-demand parent tips on issues such as cyberbullying, sexting, and online privacy. There were more than 1.5 million views of our video parent tips on these platforms in the first eight months of this year.
- Last month, 12,000 parents participated in an online event hosted by Common Sense Media and Nickelodeon's ParentsConnect, where we answered parent questions around cyberbullying and kids' online safety.

Concern about online privacy is also growing among policymakers – in Washington, DC and in the states. In addition to this important hearing, I've participated in or attended several Town Hall events in California in recent weeks where Congressional leaders addressed online privacy, safety, ID theft, and other issues. I'll participate in another next week in Los Angeles with California Senate Majority Leader Ellen Corbett.

II. The COPPA Proposal

The FTC's COPPA proposal represents a significant step in updating protections for children online.[5] The FTC's thoughtful and reasoned approach reflects the reality of some present threats to children's privacy. Now more than ever, kids are using mobile devices with the capability to reveal their precise location. Further, the FTC's handling of IP addresses and other identifiers strikes a balance between maintaining the internal operations of online services and protecting children from intensive tracking and behavioral advertising.

a. Mobile & Location Updates

It is especially valuable that the FTC has clarified that COPPA covers online services on mobile platforms.[6] The Commission's proposal to also include geolocation information under the definition of information protected by COPPA further updates the rule to reflect the current electronic and digital world. Online services and operators no longer collect just traditional street addresses, but also Global Positioning System data and other indicators of location that can be just as accurate, if not more so. Importantly, while users may actually enter their street address information into a service, geolocation information may be collected by a service with little or no user knowledge.

The ability to track the mobile whereabouts and habits of an individual as she or he moves throughout our society raises hyper-sensitive privacy concerns. Privacy is an issue everywhere in the electronic world, but mobile privacy is an issue on steroids.

For kids, this is absolutely critical – knowing what a child or teen does online at home is one thing. Knowing where they go after school, with whom they visit, and what they search for is not only incredibly invasive, it is potentially very dangerous and a fundamental violation of

[5] Federal Trade Commission, Children's Online Privacy Protection Rule, 76 Fed. Reg. 59,804 (Sept. 27, 2011) [hereinafter COPPA NPRM].
[6] *Id.* at 59,807.

their personal privacy and self-interest. Mobile companies and app developers that have a cavalier attitude about this topic need a very clear wake-up call. Common Sense believes all users should have "opt-in" protections for location information for all mobile services and apps, and it is especially important to protect children and teens.

Several recent surveys reinforce concerns about mobile technology and geolocation:

- In a survey by TRUSTe, 77% of smartphone users said that they don't want to share their location with app owners and developers.[7]
- In a Nielsen survey of mobile subscribers who recently downloaded apps, 59% of women and 52% of men said they are concerned about their privacy when using geolocation services and check-in apps.[8]
- The Future of Privacy Forum analyzed the top 30 paid mobile apps across the leading operating systems (iOS, Android, & Blackberry) and found that 22 of them – nearly three-quarters – lacked even a basic privacy policy.[9]

It's also important to note that mobile privacy isn't a concern just for parents, but also for teens. The Common Sense/Zogby poll also found that 81% of teens say search engines and social networking sites should not share their physical location with other companies without their specific authorization.[10]

---

[7] TRUSTe, *Survey Results Are In: Consumers Say Privacy is a Bigger Concern than Security on Smartphones*, (April 27, 2011), http://www.truste.com/blog/2011/04/27/survey-results-are-in-consumers-say-privacy-is-a-bigger-concern-than-security-on-smartphones/.

[8] *Privacy Please! U.S. Smartphone App Users Concerned with Privacy When it Comes to Location*, NielsenWire (April 21, 2011), http://blog.nielsen.com/nielsenwire/online_mobile/privacy-please-u-s-smartphone-app-users-concerned-with-privacy-when-it-comes-to-location/.

[9] Future of Privacy Forum, *FPF Finds Nearly Three-Quarters of Most Downloaded Mobile Apps Lack A Privacy Policy* (May 26, 2011), http://www.applicationprivacy.org/?p=723.

[10] Common Sense Media, *Protecting Our Kids' Privacy in a Digital World*, 3 (Dec. 2010), http://cdn2-www.ec.commonsensemedia.org/sites/default/files/privacy_whitepaper_dec2010.pdf.

It is obvious to most of us and clearly to most parents that existing protections for online privacy are inadequate and not keeping pace with the rapid changes of our mobile electronic world.

b. No Behavioral Profiling of Children.

The Commission should also be praised for its straightforward application of COPPA to IP addresses and identifiers when used for "amassing data on a child's online activities or behaviorally targeting advertising to the child."[11] Common Sense Media has consistently called for limits on behavioral profiling of kids, and the COPPA update makes clear that behavioral profiling of children should take place only with parental consent.

Children and teens should not have their online behavior tracked or any other personal information about them collected, profiled, or transferred to other parties. Without parents or kids knowing it, companies collect, store, and sell information about what kids do online and on mobile phones. Companies can install "cookies," "supercookies," or other devices that track which websites kids visit, including which pages they look at; what searches they make; which videos they download; who they friend on social networks; what they write in emails, comments, or instant messages; and more. The Commission's proposed rule change is correct, and necessary – behavioral profiling of children is wrong, especially without parental consent.

III. Legislation Is Needed to Enable Adolescents to Protect Themselves

While the proposed updates from the Federal Trade Commission will be an important step for younger kids, adolescents still need protection, and legislation has been introduced that would provide a strong baseline. This legislation also addresses an important gap in industry self-regulatory efforts.

[11] COPPA NPRM at 59,812.

H.R. 1895, "The Do Not Track Kids Act" foresaw many of the changes that FTC proposed in its COPPA NPRM, but also provides important new protections for adolescents. Teens would receive protections from behavioral marketing.[12] Further, operators of teen websites would have to provide a Digital Marketing Bill of Rights for Teens.[13] These rights would be modeled on principles of Fair Information Practices. Teens' geolocation information is protected, and they are included under the proposal for an "eraser button."[14] Contrary to the misleading description by some critics,[15] these protections would empower teens without imposing the COPPA model of verified parental consent on teens.

H.R. 1895 also picks up where current industry self-regulatory efforts fail – at protecting youth. The current Self-Regulatory Program for Online Behavioral Advertising offers no protections for adolescents, and offers children under 13 the mere promise that participants will follow COPPA.[16] The principles treat children's data (but not teens') as "sensitive data" and then promise:

> Entities should not collect "personal information," as defined in the Children's Online Privacy Protection Act ("COPPA"), from children they have actual knowledge are under the age of 13 or from sites directed to children under the age of 13 for Online Behavioral Advertising, or engage in Online Behavioral Advertising directed to children they have actual knowledge are under the age of 13 except as compliant with the COPPA.[17]

---

[12] Do Not Track Kids Act of 2011, H.R. 1895, 112 Cong. §4.
[13] *Id.* at §5.
[14] *Id.* at §6, § 7.
[15] Stephen Balkam, *Not Backing Kids Tracking Bill*, Huffington Post, Jul 18, 2011, http://www.huffingtonpost.com/stephen-balkam/kids-tracking-online_b_901974.html.
[16] See http://www.aboutads.info/.
[17] *Self Regulatory Principles for Online Behavioral Advertising*, 16, 17. (July 2009), http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf

The caveats and conditions mean that, without the COPPA update to include behavioral profiling information, much behavioral profiling can still occur so long as it is "compliant with the COPPA."

Media and technology companies can and should play a crucial role in helping families manage the role of media in children's lives, and in helping prepare teens to use media and technology in smart, responsible ways. This is especially true when it comes to protecting privacy and personal information, because these companies are in the best position to develop better technology, tools and information for users. There have been some valuable steps by industry leaders recently, such as the Do Not Track browser tools developed by Mozilla, Apple and Microsoft (although it remains to be seen whether advertising networks and data brokers will respect Do Not Track signals sent by users.) However, on the whole, efforts by media and technology companies to provide better solutions have been few, and disappointing.

At the very least, users should get better disclosure from online services and operators about their privacy policies and practices. In the Common Sense/Zogby survey, 91% of parents (and 81% of teens) said they would take more time to read terms and conditions for websites if they were shorter and written in clear language.[18] Companies may feel they must have lengthy, legal privacy policies and terms of services, but these are clearly not the best way to truly inform users – parents or teens – about data a site will collect, and how that data may be used.

At the recent F8 Developers Conference, Facebook CEO Mark Zuckerberg said "[i]n the world we're building, where the world becomes more transparent, it becomes more important for people to be good to each other."[19] This is a cynical statement where children's

[18] Common Sense Media, *Protecting Our Kids' Privacy in a Digital World*, 4 (Dec. 2010), http://cdn2-www.ec.commonsensemedia.org/sites/default/files/privacy_whitepaper_dec2010.pdf.
[19] *Facebook Offers New Vision at F8*, Politico Morning Tech, Sept. 23, 2011, http://www.politico.com/morningtech/0911/morningtech312.html.

lives are concerned. Common Sense strongly agrees about the value of transparency in terms of privacy policies and practices, and requiring companies to provide full disclosure about their privacy policies and practices would be a great place to start.

IV. Conclusion

Like our society as a whole, Common Sense Media admires and embraces the innovations that media and technology companies have developed in recent years, and we want children and families to be able to access all the benefits of these innovations. However, we also recognize some of the potential downsides of these technologies – especially for children.

All of us – parents and families, schools, companies, and policymakers – play a role in helping children benefit from these media and technology innovations, while also ensuring that they are protected from potential downsides.

Parents and families obviously play the first and most important role in protecting children's privacy, but media and technology companies can do a lot more to help them, by providing better solutions, clearer information and better tools.

Schools can and should do more to prepare children and teens with "rules of the road" for the digital world – but many schools and educators are not yet prepared to teach Digital Literacy and Citizenship, and to provide guidance about new technology in our lives. Former FCC Commissioner Deborah Taylor Tate, a member of the Common Sense Media Board of Directors, recently described the challenge:

> ...parents and schools are also struggling with social networking and its impact on education. Educators are being called on to be everything from online referees to cybersecurity experts. Most teachers are now teaching a subject that was not even part

of their college training, across mediums that had not even been invented, to prepare our children for competing in a global job market.[20]

Media and technology companies are especially important, because they are well positioned to bring real solutions – tools that are easy to find and use, and information that enables parents and teens to make smart choices.

Policymakers play a crucial role as well, as demonstrated by the recent leadership of the Federal Trade Commission regarding the COPPA rules. This Congress should demonstrate similar leadership, by urging media and technology companies to innovate to protect online privacy, and by building sensible legislation that will empower parents and teens, protect children, and preserve privacy in a thriving electronic economy.

Thank you again for this important hearing, and for the opportunity to speak with you today.

---

[20] *Schools Enter Digital Conversation*, Nashville Tennessean, Sept. 21, 2011, http://www.tennessean.com/article/20110922/OPINION03/309220019/Schools-enter-digital-conversation?odyssey=mod|newswell|text|Opinion|p

common sense media

Protecting Our Kids' Privacy in a Digital World

A Common Sense Policy Brief

December 2010 / Common Sense Media

Common Sense Media
650 Townsend Street
San Francisco, CA 94103
☎ 415.863.0600
www.commonsense.org
www.facebook.com/commonsensemedia
www.twitter.com/commonsensenews

Common Sense Media is dedicated to improving the lives of kids and families by providing the trustworthy information, education, and independent voice they need to thrive in a world of media and technology.

Go to **www.commonsense.org** for thousands of reviews and expert advice.

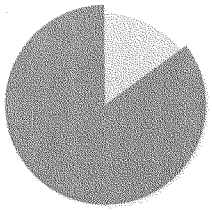
Most kids today live their lives online, immersed in a mobile and digital landscape. This brave new world has revolutionized childhood. Kids and teens now create and consume enormous amounts of online and mobile content. Their access to people and information presents both possibilities and problems. While the Internet is a platform for innovation and economic growth and brings rich resources for entertainment and learning, the very nature of digital interaction creates deep concerns about kids' privacy.

Today, our kids are growing up in public. Whatever they text or post can be searched, copied, pasted, distributed, collected, and viewed by vast invisible audiences. Parents rightly fear that their children's activities and personal information are being tracked and traced.

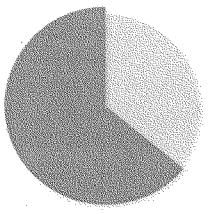
Tracking and profiling children online has quickly become a widespread practice. *The Wall Street Journal* recently found that 4,123 cookies and other pieces of tracking technology were installed on a test computer that was used to visit the top 50 websites for children and teens – 30% more than a *Journal* test of the top 50 overall sites, which are generally aimed at adults.

So what privacy protections do our children have – and what protections should they have? At the moment, there's mainly a law written in 1998, when Google was just beginning and Facebook and Zynga didn't exist. The Children's Online Privacy Protection Act (COPPA) prohibits the collection of "personally identifiable" information – including name, phone number, email or street address, and Social Security number – from children ages 12 and under without parental consent. COPPA remains the cornerstone policy protecting children's online privacy, but the technological advances that have occurred since 1998 make COPPA woefully out of date for keeping children safe from new threats to their privacy.

This brief lays out principles for a new public policy agenda to protect the privacy of children and teens online.



85% of parents say they are more concerned about online privacy than they were five years ago. Common Sense/Zogby Survey, 2010



61% of parents say Congress should update laws related to online privacy and security for children and teens. CSM

principle 1

Do Not Track Kids

Children and teens should not have their online behavior tracked or any other personal information about them profiled by third parties or transferred to third parties. The 1998 COPPA categories of "personally identifiable" information (e.g. name and address) must be updated to include other "persistent identifiers" and to encompass all of kids' online activities. What children and teens do online should remain private.

Companies – whether Internet service providers, social networking sites, third party application ("app") providers, data-mining companies, or advertising networks – should not be permitted to sell or transfer that personal information.

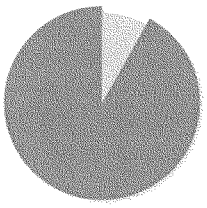
principle 2

The Eraser Button – Parents and Kids Should Be Able to Delete Online Information

Children and teenagers should have the opportunity to delete information they have provided about themselves. Too often we hear about young people who post information they later regret and find they can never fully delete from the online world. Children post personal information on websites, virtual worlds, social networking sites, and many other platforms. Children also make mistakes.

Web companies should develop tools that make it easier for young people – or their parents – to completely opt out and delete this information. Technological innovation in the online industry over the past decade has been truly amazing; the industry should apply that same spirit of innovation to creating solutions like an "eraser button" so that no 15-year-old has to live the rest of his or her life with the consequences of a poor decision about what to post online.

This is the very least we should expect from a technology industry that has repeatedly created new ways to challenge accepted norms of privacy and human behavior. Their ingenuity and resources can certainly build eraser buttons that maximize the ability to erase personal information.



94% of parents

(and 92% of teens) say they should be able to request the deletion of all their personal information held by a search engine, social network, or marketing company after a specific time period. CSM

principle 3

No Behavioral Marketing to Kids

Today many companies troll the Internet to collect our kids' detailed information in order to target them with "behavioral marketing" – advertising that is specifically tailored to their age, gender, interests, and activities. Behavioral marketing to kids is unfair and deceptive, and it should stop now.

Without parents or kids knowing it, companies collect, store, and sell information about what kids do online and on mobile phones. Companies can install "cookies" or other devices that track which websites kids visit, including which pages they look at; what searches they make; which videos they download; who they "friend" on social networking sites; what they write in emails, comments, or instant messages; and more. And thanks to new "geo-location services," companies can now also track where kids go in the physical world as well as the virtual one.

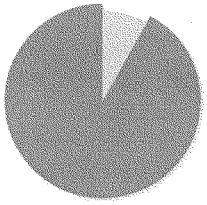
In addition, kids should not be made into marketers themselves through "viral marketing" strategies. Many sites aimed at kids now promote their content by offering kids access to special games or rewards if they email a web link to their friends – who are then invited to visit the site. It's hard enough for parents to protect their own kids' privacy without also having to worry about other kids sharing friends-of-friends information in exchange for online rewards.

Some online tracking is a helpful aspect of Web 2.0 technology, and parents or teens should be able to "opt in" to limited use of tracking devices, as long as they are not used for behavioral marketing and are not transferred to third parties. For example:

Site-specific cookies that are designed to offer users a smoother experience on the website, such as remembering a password for future site visits, pausing a game online, or remembering what's in a user's shopping cart.

Sharing their email address if they want to receive newsletters, sports scores, or other notifications from a website. However, Web operators should use the email address only for the specific purpose the kid signed up for – not transfer it to a third party or use it for behavioral marketing.

Use of location-based applications. Companies should continue to be able to provide location-based applications to children with parental permission and to teenagers who opt in. However, location-based information about children and teens should not be stored, transferred, combined with other data, or used for behavioral marketing.



91% of parents

(and 81% of teens) say search engines and social networking sites should not share their physical location with other companies without their specific authorization. CSM

principle 4

The Industry Standard for All Privacy Should Be Opt In – Especially for Kids

Companies and operators must make significant changes in the ways that they collect and use kids' personal information. Most importantly, the industry standard should be "opt in" – in other words, companies and operators should not collect or use personal information unless users give explicit prior approval.

The opt-in standard is fundamental to our ability to control our personal information. If online companies, services, and applications want to collect and use personal information, they should get permission beforehand by asking people to opt in to the service.

Too many online companies launch new services -- such as location-based applications – and enroll users automatically, giving them the opportunity to opt out afterward. This can mean that a kid's personal information is collected and used before the kid or the parents even understand how the service works. All online companies, services, and third-party application providers should follow an industry standard of getting an opt in, especially for kids.

principle 5

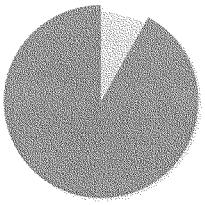
Privacy Policies Should Be Clear and Transparent

Privacy policies need to be easy for users to find and understand and should be carefully monitored and enforced. Any significant privacy policy changes should require a clear new opt in by the user – or the parent, depending on the age of the child.

We all want instant access to online content and are often too quick to click the "I accept" box to get where we want to go. For young children and teenagers, the impatience and temptations are probably even greater, and the risks posed to their privacy may seem further removed.

Most privacy policies today are lengthy legal documents written at a college level or beyond. Instead, companies should use icons and symbols that would be easy to understand and would clearly convey how users' personal information will be used.

In addition, some sites have one privacy policy for the site itself and other policies that apply if users click on an application or advertisement, resulting in complex layers of legalese that are virtually



91%
of parents

(and 81% of teens) say they would take more time to read terms and conditions for websites if they were shorter and written in clear language. CSM

impossible to follow. We need clear, succinct language for privacy policies. We also need third-party ratings of privacy policies so that parents and kids can get independent information about how policies work.

Online providers should also be held accountable for monitoring and enforcing their privacy policies. Far too many breaches of websites' privacy policies have been allowed to occur. For example, a *Wall Street Journal* investigation revealed that many Facebook applications – including the 10 most popular ones – sent users' unique Facebook IDs to outside advertising or data mining companies, even if the user's Facebook account had been set to "private." According to Facebook, this was a violation of the site's own rules. Companies that build their business on people sharing personal information need to ensure that they can fully protect that information and enforce their own policies.

principle 6

Parents and Children Should Be Educated About Online Privacy

Kids and their parents need to do their part to protect their online privacy – and the privacy of their friends. We need a large-scale, multi-year public education campaign to help them learn how to do so effectively, and it should be funded by industry.

While this brief outlines steps that industry and policymakers should take to protect children's privacy online, it is also important that families take responsibility for protecting their privacy themselves. Young people need to learn to protect their own privacy and to respect others' privacy.

The online/mobile world is changing so rapidly that children, teachers, and parents all need to be educated about online privacy. There should be a digital literacy curriculum in every school in this country, with privacy as an essential component of that curriculum.

principle 7

Privacy Protections Should Apply Across All Online and Mobile Platforms

Many kids today don't go online – they always are online, whether from their home computer, cell phone, or Web-connected video game player. For the same reason, current privacy regulations need to be clarified and applied to all online and mobile services and platforms. Social networking sites shouldn't be able to collect or sell kids' private information, and neither should third-party apps on those sites. Location-based services shouldn't be allowed without prior consent, regardless of whether the service is provided by a non-FCC carrier.

Conclusion

As a nation, we need to protect the privacy of children and teenagers in the mobile and online worlds in which they live by building on several key principles:

1. Do Not Track Kids
2. The Eraser Button: Parents and Kids Should Be Able to Delete Online Information: Easy-to-use "eraser buttons" will let parents or teens fully delete information they no longer want online.
3. No Behavioral Marketing to Kids: Children and teens should not be targeted using their online personal information.
4. The Industry Standard for All Privacy Should Be Opt In – Especially for Kids
5. Privacy Policies Should Be Clear and Transparent: Privacy policies need to be easy for users to find and understand and should be carefully monitored and enforced.
6. Parents and Children Should Be Educated About Online Privacy: A major new privacy education program will help parents and kids do a better job of protecting their own and others' privacy.
7. Privacy Protections Should Apply Across All Online and Mobile Platforms: Privacy protections should apply to all platforms – including laptops, cell phones, and Web-connected video game consoles – and to all providers, including apps, ad networks, and websites.

Children's online privacy addresses two key American concepts: our fundamental right to privacy and our need to protect our children from potential harm. The extraordinary technological changes and new mobile and social media platforms that have developed in recent years have created entirely new environments for children and teens, with unprecedented implications for their privacy. It is time to update our nation's privacy policies for the 21st century. Everyone needs to be a part of this new effort: industry, families, schools, policymakers, and young people themselves. Public policy can and should lead the way to common sense solutions.

WHO WE ARE

Common Sense Media is dedicated to improving the lives of kids and families by providing the trustworthy information, education, and independent voice they need to thrive in a world of media and technology.

More than 1.6 million people visit the Common Sense website every month for age-appropriate media reviews and parenting advice. Tens of millions more access our advice and information through our distribution partnerships with leading companies like Comcast, DIRECTV, Verizon, Time Warner Cable, Cox Communications, Facebook, Yahoo!, Google, Apple, Disney, Netflix, Best Buy, AOL, Symantec, and more.

Mrs. BONO MACK. Thank you, Mr. Simpson.

And I will recognize myself, then, for the first 5 minutes of questions. And again, I thank you all very much for your testimony.

And I would ask, Ms. Engle, can you elaborate on why the Commission opted not to seek a change on the age threshold?

Ms. ENGLE. Yes. That was an issue that we considered very carefully and we thought that Congress when it enacted the statute and it also thought about that at the time and believed that it reached the right result that under 13 is the right cutoff. While any particular age cutoff is going to be somewhat arbitrary and children do develop at different rates, the whole idea behind and the way that COPPA works is for the child to provide their parents' email address in order that the operator may contact the parent to get permission to further interact with the child. And the concern is that if you raise the age, COPPA may not work well because older children may not provide the parent's email address. They may provide their own or their friend's or a sibling's. And that is true even more now than it was earlier because it is very common now for children to have their own email addresses or multiple email addresses or they may simply lie about their age. And younger kids can do that as well but it is less likely.

And finally, we have concerns about the constitutional rights that courts have afforded to teenagers and whether that might be unduly intrusive on the teenagers.

Mrs. BONO MACK. Thank you. And you mentioned the email-plus rule. So the COPPA Rule allowed Web site operators to use a low-cost email-plus approach in determining whether there has been verifiable parental consent. And this was intended to be a short-term option available only until the Commission determined that more reliable consent methods had adequately been developed. Has the Commission now made such a determination and do sufficient substitutes for email-plus currently exist? And if you disallow that mechanism immediately, does that leave businesses in the lurch?

Ms. ENGLE. So the Commission, when it crafted the COPPA Rule, decided to make a distinction between personal information collected for a site's internal use and information that is used publicly. That distinction is not in the statute itself but the Commission decided that it made sense on a temporary basis to make that distinction and allow a less reliable method of obtaining consent called email-plus assuming that more reliable methods, new technology would develop. That turned out not to be the case. The Commission expanded allowing that unreliable method a couple of times and then ultimately made it go on indefinitely when no new technologies developed. But having reconsidered it over the years, you know, we believe that COPPA statute didn't make that distinction between internal and external uses and that perhaps this unreliable but easy method has actually deterred the development of technologies that would allow a more reliable method.

So in its place we are proposing that companies can apply to the Commission for a new method if we would place it on the public record, get comment, and that would allow the Commission the opportunity to really evaluate the method and determine whether it is reliable and then essentially include it in the Rule. It is true right now that the list of reliable methods is not exclusive. Compa-

nies can use any method that is reasonably designed to ensure that the person providing consent is the child's parent, but what we heard is that companies prefer the assurance that this is the method that essentially the Commission has blessed. They want it listed. They don't want to take the risk that the Commission may find it inadequate. So we have proposed this new method to help provide that assurance.

Mrs. BONO MACK. Thank you. That is understandable.

And the FTC proposes to add factors to its "totality review" of Web sites to determine if they are targeted to children under 13—for instance, music and celebrities that would appeal to children but many celebrities and a lot of music content appeal to both 8-year-olds, 13-year-olds, and 49-year-olds. Would that blur the age line and create confusion for Web sites as to whether or not they would be considered a COPPA operator?

Ms. ENGLE. No, I think that, you know, we are still maintaining the same test basically. It is the totality of the circumstances. We look at a number of factors to determine whether a particular site is directed to kids under 13 and by adding more factors, we are not changing the test. We are just making it clear that these are factors that one can consider. And yes, it is true that it is never, you know, will never be a bright-line cutoff that no children under 13 would be interested in an over-13 site and vice versa. But by adding more factors, we are trying to make it more transparent to operators the kinds of factors the Commission considers.

Mrs. BONO MACK. Thank you. And right on time.

The Chair will recognize Mr. Butterfield for 5 minutes.

Mr. BUTTERFIELD. Thank you.

There is a published study titled "Always Connected: The New Digital Media Habits of Young Children." I believe Dr. Montgomery has referred to it from time to time. This study published through the Sesame Workshop contains some interesting findings about the digital media usage habits of white, Hispanic, and African American children. In particular, while the study points out that the digital divide remains, when children of color do have access to digital media, they tend to use it substantially more than white children. African American children between ages 5 and 9 the report says spends 41 minutes online per session. White children in that group spend 27 minutes online per session. Hispanic children between the ages of 8 and 14 spend almost 2 hours online each day. That is 40 minutes more than white children. The study also points out that children from low-income and ethnic minority homes are less likely to have adult guidance when accessing the Internet. As a result, they are spending more time on lower-quality Web sites or on activities that won't help them develop school-based skills.

And so, Dr. Montgomery, I would like to hear any thoughts that you might have whether COPPA parental notice and consent models work well for all children or if there are any changes that could and should be made to account for the differences that I have referenced.

Ms. MONTGOMERY. Yes, thank you for asking that. I am concerned about ethnic children as you point out and I am actually looking at a lot of those issues in another context. I am doing a project on food marketing and we are very concerned that there are

very aggressive techniques that are being used to target particularly ethnic children who are at greater risk for obesity as well. So this is a very complicated problem.

I think it is probably difficult to enact a law that can address those specific needs around privacy. What we want to do is to have a set of rules that work as best as they can for all children with special sensitivities to children who are at risk. And I think that the proposed changes in the guidelines will do that, but it is going to be very important that companies take these obligations very, very seriously. And particularly, I think companies that are targeting that age group ought to be encouraged to develop their own self-regulatory mechanisms to work more effectively to ensure children's privacy.

Mr. BUTTERFIELD. But you do agree this is an issue that we need to be concerned about and address?

Ms. MONTGOMERY. It is.

Mr. BUTTERFIELD. As best we can legislatively.

Ms. MONTGOMERY. And not only that. Spanish language needs to be looked at. I think that the Congress could do more to look into these things. We haven't had enough examination of these areas either.

Mr. BUTTERFIELD. Ms. Engle, has the Commission looked at this issue in any respect?

Ms. ENGLE. The Commission has not received specific data on—I mean we do have information on the greater use of Internet technologies and mobile technologies certainly by ethnic minorities for example. Whether there are additional protections that are needed that come from that, we haven't received information on that.

Mr. BUTTERFIELD. Do you agree with Dr. Montgomery that it might be a little difficult to develop some type of regulatory protections to protect against these, that ideally it is a problem but developing protections might be challenging?

Ms. ENGLE. Yes, I agree with that.

Mr. BUTTERFIELD. All right. Can you help us out, Mr. Simpson, with this, please?

Mr. SIMPSON. Well——

Ms. MONTGOMERY. Can I add something?

Mr. BUTTERFIELD. Yes, sure.

Ms. MONTGOMERY. Because I do think in one area that we might want to think about changing some things because if we look at the kinds of data that are collected, when racial data are collected and children are then marketed to based on the kind of profiling that can take place with that data, that I think can be very problematic and can be very discriminatory and I think that needs to be investigated.

Mr. BUTTERFIELD. All right. Mr. Simpson?

Mr. SIMPSON. The only thing I can really add, sir, is that one of the concerns we see in the broader space around privacy and other concerns that parents have around digital media is it is, as the FCC's studies have shown, one of the reasons for lack of adoption of broadband and digital media. We all see great benefits for families and communities in broadband and what it can bring to their communities, but if they are reluctant because of what they see as the downsides—and lack of privacy and security is certainly one of

them, especially in rural areas and among low-income communities.

Mr. BUTTERFIELD. Let me give my last 5 seconds to Mr. Reed. Yes. Yes.

Mr. REED. I want to be the guy with good news here. I am sure that you have seen studies from Danah Boyd and more importantly, we have worked with Dr. Nicol Turner-Lee at the Joint Center and it turns out that mobile applications and the mobile environment is something that actually is having an impact in low-income and especially minority communities. And I think as we talk about privacy and what the government can do to shut down things and be careful about it, I think it is really important that we allow some opportunity for these things to flourish. Remember, mobile apps have only been in existence since 2008 and what we have seen from Dr. Nicol Turner-Lee's information and Dana Boyd is there is a huge opportunity for us to reach people who have never had a PC in their home through their mobile phone, but more importantly, their mobile smartphone. So I think as you talk about what the government can do and the ways it can play a role, we need to make sure that the choices are there for them to have cool things to do rather than just tell them how they can't do things.

Mr. BUTTERFIELD. Thank you.

Mrs. BONO MACK. Thank you.

The Chair will recognize Mr. Barton for 5 minutes for questioning.

Mr. BARTON. Thank you, Madam Chairwoman.

I am going to ask my first question to the representative of the Federal Trade Commission.

If you don't expand the protections of the law to 13- to 17-year-olds explicitly, how do we protect them? Because they are not adults and while they are able to make some decisions on their own, I do not know that they are fully capable of making some of the decisions that would be required in this area.

Ms. ENGLE. The Commission is considering the privacy interests of teens in its broader review of privacy generally and certainly we have considered that. Some of the ideas that we have offered in that area, for example, very clear notice about the kinds of information that is being collected and how it is being used made at the point that the information is collected as well as data security would also provide benefits to teens. But the Commission at this time hasn't reached any conclusions as to what additional privacy protections teens may need.

Mr. BARTON. So would it be safe to say that the provision in the Barton Markey bill that gives these protections explicitly to 13- to 17-year-olds, the FTC is not automatically opposed to; you are just not totally supportive of? Is that a fair statement?

Ms. ENGLE. The Commission hasn't taken a position on the legislation yet, but I would say that we are definitely not automatically opposed to it and we would be happy to work with you on it.

Mr. BARTON. In a similar vein, in the bill that Mr. Markey and I have introduced, we explicitly cover mobile applications. The proposed enhancements that you testified to in existing law do not explicitly cover mobile applications. Are you opposed to the provision

in the Barton Markey bill that makes that explicit or you just need to study that more also?

Ms. ENGLE. No, we are not opposed to it. In fact, we believe COPPA already does cover mobile applications. We interpret them to be online services already covered by the Rule, and in fact we recently brought a case against a company that was a mobile app provider on that basis.

Mr. BARTON. See, my position is that more and more of our teenagers and certainly even, sadly, children are getting iPhones and iPads and you almost have to explicitly cover mobile applications just because that is where the younger generation is going. So, you know, they are not going to be sitting behind a computer. They are going to be walking around and doing stuff as they are out and about.

I want to ask Mr. Balkam, your institute has got a great-sounding name. Who funds that? Who funds your institute?

Mr. BALKAM. We have more than two dozen members mostly from industry, so from AOL at one end of the alphabet to Yahoo at the other.

Mr. BARTON. And there is nothing wrong with that, but they would be industries that try to make a profit—which again is a good thing—by using the Internet and they would tend to want to collect information about people on the Internet. Is that not a fair statement?

Mr. BALKAM. I think that is a very fair statement and I also agree with my colleague Nigam's point that it would be against their very own interest to, as it were, violate kids' privacy in so doing because it would actually rebound against them.

Mr. BARTON. OK. Now, my understanding is that your institute doesn't support the bill that Mr. Markey and I have introduced, is that correct?

Mr. BALKAM. That is correct. I particularly took notice of the eraser button idea and particularly Congressman Markey's own statements at an Internet privacy hearing in July when as he was talking about kids posting stuff—particularly teens—I will quote him, "what were they thinking? It will want to be the parents who will want to erase it. They have a right to do so. I am not talking about Big Brother; I am talking about Big Mother and Big Father." And so given that, while proponents of the bill talk about giving kids and teenagers more control over their privacy, what we see—and particularly let us think about a 17-year-old who is already——

Mr. BARTON. I want to ask you one more question. I am not going to cut you off but I have only got 20 seconds so——

Mr. BALKAM. We have serious concerns about parents taking things off the Internet of their 17-year-olds and it is not as simple as rubbing out like a piece of——

Mr. BARTON. We can work on that. I want to get consensus on one thing I think that your group can agree with me on. Do you oppose the use of super cookies, your group?

Mr. BALKAM. We think that it is something that deserves considerable amount of attention and we are looking forward to future hearings on that, yes.

Mr. BARTON. OK. Well, for those of you that don't know, a super cookie is something that is put on your IP address without your permission and you cannot delete it. You don't know about it. It can collect information—it can even collect information on where you go on other sites and you don't know anything about it and it can't be deleted. And I hope at some point, Madam Chairwoman, that we will all agree legislatively to ban super cookies. And with that, I would yield back.

Mrs. BONO MACK. I thank the gentleman.

The Chair recognizes Mr. Towns for 5 minutes.

Mr. TOWNS. Thank you very much, Madam Chair.

Mr. Simpson, in your testimony you emphasize companies can play a more active role in protecting privacy and personal information. In what ways can companies play a more active role in protecting our privacy?

Mr. SIMPSON. Thank you, sir. I think most importantly I would recognize there are quite a few companies that are doing a better job of providing information, but I think the most important change that companies need to make in this space, companies large and small, is better opportunities on their own platforms, on mobile apps, on all the devices that they provide so that parents in the case of younger children and teens themselves have more chance to understand what is going on; what data is being collected; how they can opt out of it; whether they should or shouldn't opt into it; and to keep that information simple, accessible, and actionable. The big challenge in this space right now is that it is very hard to find out what is going on with my data when I use a given device or platform. The easier they can make that, the more we have parents who can make informed choices on behalf of young kids and teens who can make informed choices on behalf of themselves.

Mr. TOWNS. All right. Thank you very much.

Mr. Balkam, Family Online Safety Institute is your operation, right?

Mr. BALKAM. Um-hum.

Mr. TOWNS. All right, good. What do you think the FTC did right in their proposed rule and what do you think is missing?

Mr. BALKAM. Well, as I said in my own testimony, I think they got the balance just right between protection on the one hand while not squashing innovation on the other. I don't think that there was anything that they left out. I mean it was quite a thorough review. We are very impressed with the range in their technical know-how about emerging technologies. So we are pretty happy with it.

Mr. TOWNS. What about the definition of a child's age?

Mr. BALKAM. We think that is appropriate. We certainly do not advocate for it to be increased. As I was beginning to explain in my last response, we have some serious concerns about the older teens and whether or not they have some rights of free speech themselves. We don't really see the need for parents to come in and to take away their content as it were.

Mr. TOWNS. All right. Thank you very much.

Ms. Engle, you know, there has been some questions about the response period and the notification and that people are not informed. What methods and techniques do you use to solicit responses?

Ms. ENGLE. Are you referring to comments on our proposals?

Mr. TOWNS. Yes.

Ms. ENGLE. Well, we have published it in the Federal Register issued, of course, as we must with all proposed rulemakings. We issued a press release, we have reached out extensively, we have an extensive email list to privacy advocates and people who have expressed interest in privacy, you know, in COPPA over the years. We are doing a lot of speaking. In fact, one of my colleagues is up in New York this morning speaking to the Children's Advertising Review Unit Conference on our proposal in COPPA.

Mr. TOWNS. And the reason I raise this issue is that many members of the faith-based community are saying, look, nobody talked to us. We are not aware of this. When did it happen? In fact, they even blame me in many instances, you know, and that is my problem.

Ms. ENGLE. Well, I know we have done outreach to faith-based institutions in other areas, for example, in fraud protection, and I think we can look into doing that here as well.

Mr. TOWNS. Right, because these faith-based institutions have what we refer to as national conferences and if you in some way could arrange to get on their agenda, I think it would be a great service to all of us because they have some input there and I think that we should solicit it.

Yes, Mr. Reed?

Mr. REED. I just wanted to add to that. I think you really hit a key point, and Congressman Butterfield, the app that I was talking about from your district, the author of that app has raised concerns. This was the first she heard about it when I contacted her through a group of developers. And she said well, this app allows grandparents to contact kids. Do I need to get parental explicit consent? How do I go about the process? And so this entire process to her, while there are rules and regulations, the publishing of something in the Federal Register, having discussions with privacy advocates is not necessarily the same as reaching out to the faith-based communities. And specifically, the app in your district is exactly the kind of app that Congressman Ed Towns has talked to me about. And I am hoping that we can work with her to make sure she understands the changes.

Mr. TOWNS. Thank you very much, Madam Chair. Yes, thank you.

Mrs. BONO MACK. I thank the gentleman.

The Chair recognizes Mr. Harper for 5 minutes.

Mr. HARPER. Thank you, Madam Chair.

And I certainly want to thank everyone for being here and as a parent now to a 19-year-old and a 22-year-old that we dealt with those issues and we had AOL and we used age-appropriate email settings as they were growing up. You know, I think there is a large responsibility for the parents themselves to make sure that they are monitoring this and we certainly want to have those tools available.

And this is just a curiosity question, Ms. Engle, on violations that come to your attention that result in fines. Just a general breakdown of the percentage that come from your own search or investigation or policing, those that might come from third-party

organizations and those that perhaps are reported by parents, can you give me just a general breakdown?

Ms. ENGLE. I would say probably most of the violations we detect are from our own review. We do also get complaints and things are brought to our attention by the COPPA Safe Harbor Programs. They are a frequent source of complaints.

Mr. HARPER. If I could just ask this sort of as a—you know, we have heard a lot of different testimony here but just at its most basic level, what is wrong with advertising to children based on those likes or dislikes so long as the child is anonymous?

Ms. ENGLE. So we think that the same privacy interests that inspired Congress to enact COPPA in the first place, the idea that at least with respect to children under the age of 13, young children, that parents are the ones who should be in the position of making the decision of permitting their children or not to interact with a Web site. And it goes both ways, both in terms of the Web site collecting personal information from the child and also being able to contact a child individually. And what we are seeing now and what is behind our proposal is that with things like tracking cookies which are able to track children across Web sites over time and direct ads based on their web browsing activity, that that is a form of contact of an individual that falls within COPPA.

Mr. HARPER. OK, thank you.

Mr. Reed, I would like to ask you a few questions if I may. And certainly I know your position in a statement on a Supreme Court decision earlier this summer, Brown v. Entertainment Merchants Association, 7–2 Supreme Court decision that dealt with the sale of videogames to minors. Is there anything about that case that correlates to this that you have seen?

Mr. REED. Well, I think we have to step back and think to ourselves, what are we trying to do? What are the goals we are trying to achieve? I have an obvious bias. My goal is to make sure that we have mobile apps developers able to create jobs and specific applications that reach the right audience. And so when you look at both the Supreme Court decision and where we are heading both on this panel, I think it is pretty clear that our industry is, to borrow a phrase that was used earlier, putting the pedal to the metal and trying to get things into the hands of as many people as possible. Therefore, we are going to be enthusiastic and supportive of ways that allow people to have access to our technology.

That said, just like with videogames, we are very sensitive to the content question. There is a big difference between, as we have discussed, and it is an interesting part about this whole privacy regime, in interviewing parents prior to this hearing and in other cases, when you ask them what do you think when you see that "only 13 and over" in this location? The vast majority actually think it is about content, not about privacy. So I think that we have merged a lot of these privacy questions with content questions in a way that I think we need to pull back from. So when it comes to violent videogames, when it comes to Supreme Court decision, we need to maybe separate a little bit out on how we view the collection of information, the content of information, and who the audience of those are.

Mr. HARPER. And I know I am almost out of time. I want to end with one last question, Mr. Reed, if I can. You know, you had expressed some concern about the FTC's proposal to disallow the email-plus system. And I would like for you to just speak for the next 23 seconds on that.

Mr. REED. I will make it really short. We are concerned that the FTC's email-plus complete abandonment is a bit of a Hail Mary. It is a well, we will get rid of this technology and magically new technology will develop. Now, that might happen but I think we are probably better off given just exactly how nascent the mobile apps industry is and how we are quite literally learning every day that I think we probably, if we are going to do anything, it should be considered sunsetted or given a longer time to stretch it out a little bit because I am not sure in the mobile space people are exactly ready to just magically create new technology out of next week. Remember, most of these companies are small and they don't have staffs of technologists ready to develop their own version of verifiable parental consent. So there needs to be some industry percolating and I believe there are other incentives that can be used rather than just tossing it all out at once.

Mrs. BONO MACK. I thank the gentleman.

I now recognize Mr. Guthrie, also the home of Oink-a-Saurus, for his 5 minutes.

Mr. GUTHRIE. Thank you very much. I have to figure out where Oink-a-Saurus is so I have to——

Mr. REED. I will send you a link.

Mr. GUTHRIE. Send a link. That would be great. Thanks a lot.

To Mr. Nigam, in your testimony you said that we don't need to be focusing on things that sound bad and focus on things that are bad. What is an example of things that sound bad that we have focused on that distracts us from——

Mr. NIGAM. I mean I will go back more into the historical Internet safety world. There was a time when anytime somebody went online there was this fear that predators were going to attack them and that sounded bad, and then once that happened, there were tons of proposals on do A, B, C, D, and E to stop that. But every time research was done, what ended up happening was researchers showing around less than 1 percent or even less than that there were actual issues with that as opposed to issues with things like digital fingerprints that kids are leaving online when they are going places and 10 years later it is going to be haunting them when they are applying to college. That is bad versus what sounded bad. So those are the kinds of things that I am referring to when talking about that.

Mr. GUTHRIE. OK. And you mentioned that it would be against the business model to abuse the information because obviously people would quit going to that business if that is the issue, but the FTC does find violations of it. Even though it would be a bad business model to do it, people are doing it or have done it, because from the FTC you do find violations of COPPA, I think. So how do you explain that?

Mr. NIGAM. I think that is a great question because if you look in the last 11 years, there has been 17 actions, which to me is amazingly small. And what you are finding if you go through each

of the 17 actions, for the majority of them what you are going to find is companies who are unaware, didn't have the resources, didn't have counsel advising them, hadn't done the review when the developer was creating this great idea and most of the time didn't even know they were doing what they were found to be doing, which I think is very different than saying there is a company who made an executive decision. We know there is COPPA, let us see if we can get away with it, and we will make $10 million by the time they figure it out, and we will be disappearing after that.

Mr. GUTHRIE. So there are no kinds of cases of that like you see in Medicare fraud or stuff like that?

Mr. NIGAM. I haven't read every line of everyone, but I would——

Mr. GUTHRIE. You know of no case that does that?

Mr. NIGAM. If there is, I am not aware of it.

Mr. GUTHRIE. The typical violator would be someone who you find are small businesses that just, "Well, I didn't know I was supposed to do that" kind of thing?

Ms. ENGLE. No, actually many of our cases are again very large companies—Sony BMG, Universal Music Group, Iconix, but what we have found in those cases is they attempted to comply with COPPA but didn't really follow through. So they may have at the registration page asked for someone to enter their date of birth and they intended that if the person entered an age under 13, they would be kicked off. In fact, they weren't. And then those kids were able to post information, et cetera.

Mr. GUTHRIE. OK.

Mr. NIGAM. If I may.

Mr. GUTHRIE. Yes, go ahead.

Mr. NIGAM. And having worked inside the companies with developers, what you often find happening is legal counsel in the large companies, most say here are the requirements. Developers don't always understand that and there is where the disconnect occurs. So when something is executed, you create a new product, a new feature, it may be one of those left-behinds or the right process wasn't in place, which is very different than an intentional violation or attempt to collect information from children that you know would violate their privacy rights or violate COPPA for that matter.

Mr. GUTHRIE. Professor?

Ms. MONTGOMERY. Yes, I just wanted to say that having observed this all from the very beginning, if we hadn't instituted COPPA, you would see a very different marketplace. It is not a question of a business model not working. It wouldn't work now because it is not legal to work in that way, but it was heading in a direction that would have been absolutely outrageous and we would all be very, very upset at what we saw because data collection was built into the heart of it. And that is also what is happening with teens and adults as well. So that is why I think we need safeguards for everybody.

Mr. GUTHRIE. Thanks.

Mr. NIGAM. And I do agree with what was just said in the sense that the expectations have been established and it has had a tremendous impact on the marketplace and the way it exists today.

And so when I am focusing on what do we do next, that is when we have to look at each individual proposal and say is it proposing to solve a problem that sounds bad or actually is bad? Is there gaps? Are there things that can be done and are there going to be unintended consequences? For example, shutting off email plus is a great example of that. Companies have been doing email plus with millions of users for, say, 11 years or 10 years and all of a sudden that function disappears? What do you do with that millions of users on your site? How do you recreate the process? Are they grandfathered in? Those are the questions that have to be asked in that category of is there technical implementation concerns? Will there be unintended consequences?

And I think that is why I wanted to focus more today on providing a framework within which to look at it as opposed to let us go line by line right now in this 2 hours that we have and come up with the answers.

Mr. GUTHRIE. Thank you. I yield back. My time has expired. I yield back.

Mrs. BONO MACK. I thank the gentleman and now recognize Mr. Olson for 5 minutes.

Mr. OLSON. I thank the Chair and I want to welcome the witnesses. And thank you for coming here today and giving us your time and your expertise.

And my question is for you, Director Engle. And you stated in your written testimony that the Commission is not aware of any operator directing online behavioral advertising to children. However, the Commission is proposing adding to the list of what constitutes "personal information persistent identifiers." For example, numbers held in cookies, user IDs, IP addresses, as well as screen and user names. And you state in your testimony that the effect of these additions would be "to require parental notification and consent prior to collection and use of persistent identifiers for purposes such as behaviorally targeting advertising to children."

My question for you, ma'am, is if the Commission isn't aware of any online companies directing behavioral ads to kids, then why does the FTC feel so strongly about wanting to change the COPPA Rule to address this issue?

Ms. ENGLE. Our testimony is that no individual company has admitted that they are behaviorally targeting children under the age of 13, but there have been widespread reports in the press, for example, Dr. Montgomery referred to the Wall Street Journal article earlier that reported dozens and dozens of tracking cookies placed on child-directed sites. So it appears that the industry position has been that self-regulation is sufficient here to address the problem or the issue but our thought is that, I mean, what the regulatory principle says that their members will not behaviorally advertise to children under the 13 except in compliance with COPPA. And so that actually doesn't say much because if COPPA doesn't cover it, then they are free to do it. But the outward statement appears to be that they won't do it. So we want to kind of close that gap and require parental permission before that occurs.

Mr. OLSON. OK. Mr. Simpson, it seemed like you had some comments. Do you want to follow up on that at all, sir?

Mr. SIMPSON. I would echo those remarks and say that we are seeing signs of what is increasing. We saw it in the Wall Street Journal story, we see it in the increase in ID theft, and we see it as a basic business principle of some of these companies, as Dr. Montgomery talked about, the pattern of advertising towards kids before COPPA was established. We also need to keep an eye on what the pattern of valuation of companies in Silicon Valley is right now and that is eyeballs. Do they have people on their sites? None of these companies I would suggest want to turn anyone away, and so their opportunity to reach out to kids of any age is valuable to them.

I respect what some of my colleagues have said about the importance of corporate responsibility here, but I think they are caught in a tension and they do want the biggest audience they can get, whether that is an individual app or a large Web site. So we see lots of signs of how much they are marketing toward kids and targeting kids under 13 and over.

Mr. OLSON. Yes, sir. OK.

One more question for you, Director Engle. For the 5 new proposed rule changes to the COPPA Rule being put forth by the FTC, has the Commission conducted any kind of economic impact analysis on these proposals, and if not, will you?

Ms. ENGLE. We have certainly considered the cost as well as the benefits that we hope to achieve by the rule changes, and in our Federal Register Notice, we have estimated costs on small businesses and we are specifically seeking comment on our estimates. And if we are, you know, off on our estimates and inaccurate, we certainly would like to hear from businesses about that.

Mr. OLSON. And Mr. Reed, you are representing the app world so to speak and I want to say, by the way, while I was sitting here I texted my 14-year-old daughter and told her I was with the app guy and she basically said, Dad, can I get a job with him in the future?

Mr. REED. We are hiring.

Mr. OLSON. Do you agree with that assessment? I mean the small businesses that you represent be involved in the process?

Mr. REED. I have found the FTC to be towards me—as a trade association based in Washington, D.C.—very responsive. I think that they lack the manpower and resources to really reach out to a community that is now over 100,000 developers in the larger picture and tens of thousands of developers in the educational app space. So I think that I respectfully say that we will be filing comments with the NPRM specifically about the small business impact and we look forward to working with the FTC to make sure their estimates are appropriate. I think that as we think about all of this, we have to remember 2008 was when we had our first app store. So we have had all of these changes in business models, in technology, in capabilities in 24 months. So we are looking forward to working with the FTC, and I think I am probably going to say that we are going to estimate their cost up and encourage them to take a very measured approach on the impact to small business.

Mr. OLSON. Yes, sir?

Mr. NIGAM. I just wanted to make a comment. Because of the company that we have in terms of consulting with online busi-

nesses, we spend countless hours talking about COPPA and whether to choose even going under 13 and over 13 and the eyeballs question comes up and the uniform reaction is eyeballs that are good we want; eyeballs that are going to hurt us kill our reputation, therefore kill our business. And I think that is something we should keep in mind because that goes back to companies being incentivized to find the right way to do the right thing. Now, the challenge may be what is that right thing because we can't understand what it means. That is a very different question than whether you are motivated to even try.

Mr. OLSON. Thank you, sir.

I am over time. I yield back.

Mrs. BONO MACK. I thank the gentleman.

And the Chair recognizes Dr. Cassidy for 5 minutes.

Mr. CASSIDY. I got a 10-year-old, and she will take my iPhone, go to my iTunes, and she will download Angry Birds. "Dad, can I get Angry Birds?" I never recall being asked if I am over 13. I assume iTunes knows I am over 13. But as I listen to you guys, I am suddenly realizing, man, how do you empower a parent? It sounds so nice as rhetoric, but as a guy with a 10-year-old who is always on my iPhone, I have no clue how I am empowered. I am feeling very un-empowered.

Mr. REED. I can help you with that.

Mr. CASSIDY. Somebody empower me, buddy.

Mr. REED. Within most of the devices, I am happy, you know, I can grab a cup of coffee and I am happy to walk you through. All of the devices now—some of them are better; some of them are worse—have pretty granular and pretty incredible parental restrictions that you can set up. On your iPhone, there is a page that you can go to where you can say your daughter can't download. You can set it up with its own password. You can——

Mr. CASSIDY. OK. So my daughter downloads. My son who is 17——

Mr. REED. Right.

Mr. CASSIDY. Vim and vigor, full of himself. Downloads something but my 13-year-old uses it.

Mr. REED. Right.

Mr. CASSIDY. Or if I go to my desktop, my 84-year-old mother who moves in with us is on the computer, my wife is, and then my daughter. So the super cookie has a place for my mother but it tracks all the way through three generations. Now, it seems like, unless somebody is logging off, which we don't do—we reboot it—whether there is COPPA or not, it is going to be tracking whoever is on that computer, correct?

Mr. REED. That is correct. I would of course recommend that you get more mobile devices for your household. That is the clear solution here.

Mr. CASSIDY. Well, we are going that way.

Mr. REED. Get more.

Mr. CASSIDY. Yes.

Mr. REED. But yes, you are right.

Mr. NIGAM. Oftentimes I talk about how people distinguish between the online and the offline, but when you actually step back and say as a parent, how would I handle this situation if it was

in the physical world? I think those same kinds of conversations need to apply, which means a conversation—and I have an 11-year-old—of you are not allowed to do this but your 16-year-old brother is. That is part one. Part two——

Mr. CASSIDY. That assumes—think about a television. You walk by, you see the program, you have a sense of the content over a 30-minute show. You can have an entree into an online and then that entree takes you someplace far different. So the parent downloads it looks pretty benign, and next thing I know I have got, you know, $10 on my credit card bill. Now, I figured out how to stop that, but that said, I just say it takes you in places—Ms. Montgomery, I liked your testimony, so let me get your—I think you were going to say something?

Ms. MONTGOMERY. Yes. Well, what I wanted to say is I think what we need are tools that will help parents because it is baffling for all of us, and I agree with you. It is very frustrating and you can't really control where your kids are all the time, and that is why COPPA was designed to really address the business practices and really to minimize data collection. It was not set up to facilitate parental verification so that companies could collect a lot of data. It was really developed to ensure that Web sites targeting children did not collect a lot of data.

Mr. CASSIDY. But again, if my mother is on who is 84 and something is placed which begins to track and does not log out and my daughter gets on, something benign at the outset but perhaps less benign further in, I mean my mother has set the table for my daughter to be tracked, correct?

Ms. MONTGOMERY. Well, right. That is right. And that is why, you know, I mean this is an evolving marketplace and there will be more and more of that happening, as others have noted.

Mr. BALKAM. I just wanted to make a quick point that all of the major cell phone operators now offer pretty good parental controls. And in our survey that we just released a couple of weeks ago, we found that 25 percent of American families now do use that. Now, that seems like a fairly low figure, but then you compare it to the v-chip usage, which is around 15, 16 percent, that is not too bad. I would highly recommend that you also use——

Mr. CASSIDY. Yes, I have a parental control but I am sure I am not using it to the full robustness as it should be.

Mr. BALKAM. And education. We need to empower——

Mr. CASSIDY. Now, I will tell you when I look at your documentation and it says click here, once I actually read it, it was 40 pages of legalese and a lot of it was redundant. A lot of it was actually repeated. And it is like I am thinking they are trying to defeat me from reading it. Now, we laugh but——

Mr. BALKAM. Sorry, sir.

Mr. CASSIDY. —it is repeated, repeated, repeated, and some of it is totally extraneous. It makes me think that that which actually I might object to is buried deep within.

Mr. BALKAM. I feel your pain. That is all I can say.

Mr. CASSIDY. I will tell you, though, but we have got to move beyond feeling pain to actually having something where a parent can look at and say it is one paragraph, boom, this works and this does not.

Mr. BALKAM. Right.

Mr. CASSIDY. Because right now I am thinking, heck, I can't read through this.

Mr. BALKAM. But there is another factor as well, sir, that you should consider especially with apps is that what drives those parental controls in many cases is the rating that was provided for the content. In television and movies that is provided by an industry——

Mr. CASSIDY. Can I ask one more question before I run out of time, Ms. Montgomery? I read in the Wall Street Journal that if they have this interactive game and they make the tractor red, white, and blue on a patriotic holiday, people are more like to purchase something online. You realize that there is a subliminal suggestion taking place which is modifying the behavior of the person who is actually looking at the screen. Now, if that is true for an adult, this is absolutely true for my 9- and 10-year-old. How are we going to regulate this sort of subliminal molding the person who is looking at the interactive game to manipulate them into a behavior which they frankly may not be aware they are being manipulated?

Ms. MONTGOMERY. Well, these are major concerns. And I agree with you and we haven't even talked about things like neuromarketing, which is one of the trends in the industry as well, in the online industry. But this is exactly why I think we need to ensure that COPPA makes it impossible for companies to behaviorally target, to track an individual child and to create marketing that is designed for that child based on that child's behavior, psychological profiles, and other information that has been collected from that child.

Mr. CASSIDY. OK. That seems like nice-sounding recommendations, but how do we get there? I am not quite sure I know that.

Ms. MONTGOMERY. We have to keep working at it.

Mr. CASSIDY. OK. Thank you. I yield back.

Mrs. BONO MACK. Thank you.

The Chair recognizes Mr. Kinzinger for 5 minutes.

Mr. KINZINGER. Thank you, Madam Chair.

I may be the last person to ask you questions, so congratulations. You made it. Thank you for coming.

Mrs. BONO MACK. Excuse me, sir. We plan a second round, so don't let them off that easily.

Mr. KINZINGER. OK, this round. But I really appreciate you coming in and talking to us. This is very important. And I think as we, you know, here in Congress debate things like the economy and jobs and what is the proper role of government, you know, does government micromanage an economic recovery or is it the private sector, which I believe? This is a great opportunity to show how this area is an explosive market and really a bright spot in the American economy. It would be really sad to think of where we would be, frankly, without, you know, technology innovation right now as an economy. What place would we have in the world?

So I think as we go forward it is very important that we understand that there has got to be a proper balance, of course, between where the government is involved and what it does and also stamping down on the innovation of the free market. Because again if we

are going to get out of this recession, and we are, it is going to be through that free market.

So it is good to hear also from the witnesses that the FTC is working well with the stakeholders in updating our privacy rules to reflect that evolving world. As you have heard from everybody here, I am amazed at what the young folks are able to teach me about, you know, what to do with applications and stuff like that. Even though I may be one of the younger members of Congress, all I can do on my iPad right now is surf the Internet. I really don't know how to do much else. So I can go to my nieces and nephews to help me with that if they need to.

But I also want to say to me it is incredibly hard for parents to control or even know what their children are doing, and at the same time, I feel confidence, obviously, that mothers and fathers want to have that assurance that they know what is going on and things like that.

The FTC has played an important role in this regard and should continue to work with the various stakeholders to ensure children's personal information is not being collected online. More can always be done and this committee must determine and it will determine whether the FTC has enough authority to keep up with online advances, at the same time finding that balance.

My first question, though, is to Mr. Reed. As the apps become more enhanced in geolocation and social media interactions advance—and they do it at a record pace and an exponential pace, frankly—do parents have the tools to ensure that predators won't have access to their children's location? Because, to me, I see that as potentially being a very terrible story in the future.

Mr. REED. Right. That is becoming kind of a universal conundrum. How does my child share his information with his friends and not let people that we don't want to see it, see it? We are working on technological solutions, we are working on allowing kids to kind of develop their own friends list, but that has its own shortfalls. Does my 13-year-old—mine is 5–3/4 so she is not there yet—but does she know who her friends really are? The problem is is if we take a step back, we had this problem with this device called the telephone. People could call each other and say this is where I am. I will meet you behind the park or behind the baseball field. So it is really a struggle that we have on how do we take this location information that we are provided in our mobile device and somehow segregate it in a way that is different than, say, my physical telephone in my house saying I will meet you behind the baseball field.

Mr. KINZINGER. Right.

Mr. REED. So we don't have the answers. We are trying to figure it out, but I a big part of what we are doing is empowering parents to know what their kids' device does and by alerting them very clearly, hey, this is going to share your location. Are you OK with it? And in the case of most of the mobile devices, you can turn that off completely. So in mine, my daughter can't actually hit any button that charts her geolocation. And so that is what we are going to have to do.

Mr. KINZINGER. And that is good. And again, I mean in 2 or 3 years if you all are fortunate enough to come back here and talk, we are going to have a whole slew of new different questions——

Mr. REED. Right.

Mr. KINZINGER. —because there is going to be so much that we can't even begin to imagine now. And again, that is what beautiful about our innovating economy is that, you know, that is the case.

But let me ask Ms. Engle. How is the FTC approaching geolocation technologies as it relates to children? And specifically, do you believe parents are given enough information to know what an app is storing about a child and what information is being shared with other users?

Ms. ENGLE. The FTC believes that geolocation information is already covered as an item of personal information under COPPA because COPPA refers to physical location including street name and city or state and geolocation information is at least as precise as that and often more so. But what we have proposed is specifically adding geolocation as an element of personal information just to make that crystal clear.

Mr. KINZINGER. Well, thank you. And again, this appears to be a good example of where government and private sector seems to be working well together. And I yield back.

Mrs. BONO MACK. I thank the gentleman and recognize myself for the next 5 minutes.

And to Dr. Montgomery, I appreciate very much your thoughts on this and your work on this over the years. Last week, I took a trip up to Silicon Valley and I visited a number of the big firms. It was very thought-provoking and I think that what really strikes me the most is how over the years the Internet has been built on the back of intellectual property. And early on when you think about Napster and Kazaa and the peer-to-peer networking and how we have moved into other models that actually try to pay for intellectual property, do you think, I mean behavioral advertising to me, I kind of grapple a little bit with why it is bad when sometimes they are trying to monetize these new models that end up trying to pay for content.

Anybody who is a writer in the audience, you know, anybody who has ever been a part of any creative work, any longer your work is devalued because you can't get paid. And when something is out on the Internet in digital form, a master copy is a master copy is a master copy. How do you see moving forward, then, in a world where we need to try to provide decent, quality content for our children and still protect them from behavioral advertising? And you said that if we hadn't had COPPA—and I don't disagree with you—but you said it would have been outrageous what we would be living under now. How do you find outrageous and how do you see paying for quality content going forward as people are grappling with how to pay people who create valuable content for our children?

Ms. MONTGOMERY. Well, I will tell you that what I saw in the early days was leading to a business model where marketers were talking about creating personal relationships between a product spokescharacter and a child, things that nobody would ever talk about now in terms of microtargeting and targeting individual chil-

dren. And I think what we have been able to do with COPPA is allow and enable that industry to grow and flourish but by creating some guardrails, some rules of the road where we are not taking advantage of the youngest children, whereas I mentioned earlier, research shows they don't have the cognitive capacities or the psychological developmental capacities to handle these kinds of very, very sophisticated behavioral targeting and——

Mrs. BONO MACK. But there must be some positive behavioral targeting out there, too. And this is what troubles me about these discussions we have in here with privacy, with security, is all of these issues have another side to the coin where some people see benefit, others see risk, all of these. My point here is what if we wanted to do an anti-bullying campaign? That is positive. What if we want to encourage our children to go to a great university like USC or something like that? And so there are ways to target them in a positive way as well, aren't there? We are stifling——

Ms. MONTGOMERY. Absolutely. And from the beginning what we have said and I still agree with, we were never trying to eliminate marketing or advertising in this context. We think that is perfectly fine and identifying the IPs, understanding that an IP address is still now personal information, personally identifiable, that doesn't mean you can't provide contextual advertising to children. That is still very much possible. You can do all kinds of anti-bullying campaigns. They are happening online. None of this would restrict it.

What I think is important, however, is that we create some safeguards for the kinds of data collection and profiling and highly targeted and potentially very manipulative advertising that is targeted at younger children. Now, when it comes to——

Mrs. BONO MACK. And can you speak a little bit towards monetizing the delivery of quality content? This is what it is all about at the end of the day.

Ms. MONTGOMERY. It is a tradeoff. It is always a tradeoff. And yes, of course you need to monetize the content but you do that at a price. And if it is a price that is not fair to children, that takes advantage of them, then I think you look for ways to alter that business model.

Mrs. BONO MACK. Thank you very much, Dr. Montgomery.

Mr. Simpson?

Mr. SIMPSON. Just quickly to add to that, as a big believer in those incredible educational opportunities of apps, of a lot of this digital media, how do we monetize that? As much as possible we do that with the engagement and empowerment of parents. Make them part of the equation so that they know about the cyber bullying campaign that we want to promote and that they are engaged with their kids with talking about USC and other great institutions. Make them part of the equation.

Mrs. BONO MACK. Quick question—and we are trying also to get enough time to Mr. Markey so he can be here—you like the eraser button. I don't understand how that is technologically feasible. I am not opposed to the concept, but again, if it is a digital recording, if a song is out there, it is out there forever. If a photograph is out there, it is out there forever. How do you technologically think that an eraser button is possible when it is already out there in cyberspace and you can't even attribute necessarily who originated it?

Mr. SIMPSON. You are very right on that part and one of our first pieces of advice to parents and to our educational materials for kids is to make them recognize that these things can be forever and all the more reason why kids need to be very careful about what they post, what they share. But as the bill has drafted, to the degree that it is technologically feasible, the eraser button should address some of the opportunities for kids or teens, parents in the case of kids, to take down what they own.

This also gets back to what, I believe, Congresswoman Blackburn has described as who owns the virtual you. So this is also an issue of intellectual property. This is an issue of property. When we start sharing things online, they do get much more complicated. They run into First Amendment issues and they run into shared ownership. But at what point do we have tools for parents and for teens where something that belonged to me, a picture I took of myself still belongs to me and is something I can take down.

Mrs. BONO MACK. All right, thank you. I need to yield to Mr. Butterfield for 5 minutes.

Mr. BUTTERFIELD. Thank you, Madam Chair.

Ms. Engle, let me start with you. The statute contains a broad definition of personal information. It states simply that personal information means "individually identifiable information about an individual collected online" and then includes a nonexclusive list of identifiers. The FTC is also granted the authority to expand the definition to include any other identifier that the Commission determines permits the physical or online contacting of a specific individual. This is the authority that the FTC is relying on to bring the meaning of personal information into the COPPA Rule in line with the technological changes that have happened since the Rule first went into effect.

Let me just ask you yes or no. Am I correct that you are not required by the statute to determine whether changing the definition of personal information will unreasonably impede technological innovation?

Ms. ENGLE. That is correct.

Mr. BUTTERFIELD. All right. Yes or no, am I correct that you are not required by the statute to determine whether changing the definition of personal information will adversely affect interstate commerce?

Ms. ENGLE. That is correct.

Mr. BUTTERFIELD. All right. Yes or no, am I correct that exercise of this authority does not require any finding other than that the identifier permits physical or online contacting?

Ms. ENGLE. That is what the statute says.

Mr. BUTTERFIELD. All right. Yes or no, am I correct that you get to use streamlined APA rulemaking and are not required to follow the more burdensome Magnuson-Moss rulemaking process to change the definition?

Ms. ENGLE. That is correct, although we always, you know, seek comment on burdens and cost and technological feasibility, but it is not statutorily required.

Mr. BUTTERFIELD. All right. Yes or no, is this the first time in the 11 years since the COPPA rule became effective that the Commission has proposed changes to the meaning of personal informa-

tion using its statutory authority to modify the meaning of that term?

Ms. ENGLE. Yes.

Mr. BUTTERFIELD. All right. Those are my yes-or-no questions. All right. We need to use some more time.

It seems to me that when the FTC is given the ability to modify the meaning of a key statutory term like personal information, and 2) is allowed to do so following a straightforward and streamlined process, it is shown it will not abuse the authority or act hastily. It will not run wild and create chaos and unnecessary cost for businesses. I think our experience with COPPA shows the FTC can exercise this sort of authority carefully and deliberately. I hope that is a lesson all of us here can apply to the data security context as we look to move legislation in that area that is both effective and adaptable to changes in technology and expectations about what information should be protected.

This has been a good hearing, Madam Chairman. I want to thank the witnesses and want to thank you for your patience. I yield back.

Mrs. BONO MACK. I thank the gentleman and at this point I will thank the panel very much for your answers to our questions. You have been very gracious with your time. And as I said, these issues I think no more than any others have a flipside to everything that we do. And the law of unintended consequences can be very, very frightening. And with that, I am actually just stretching—you owe me. And I am happy to recognize Mr. Markey for 5 minutes.

Mr. MARKEY. Thank you. I thank the gentlelady and I thank you for allowing me as a nonmember of this subcommittee to participate. Thank you so much.

I am the House author of the Children's Online Privacy Protection Act, which Congress passed and President Clinton signed into law in 1998. It is the communications constitution when it comes to protecting kids online but we need to update it to take into account the explosive growth and innovation in the online ecosystem over the last 13 years.

I commend the Federal Trade Commission for its thoughtful and comprehensive review and for its proposed changes to that Rule, which reflect and reinforce many of the same safeguards contained in the Do Not Track Kids Act that I introduced this past May with Representative Joe Barton.

As in our bill, the Commission appropriately notes that teens should be provided with clear information about how their personal data is used and also empowered to exercise control over these uses. As in our bill, the Commission also proposes to add children's location information under the category of personal data that require a parent's permission before it is collected or used. Given the potential for this sensitive data to be misused to endanger a child, the Commission's proposal in this area is a much-needed step.

I commend the Commission for rejecting arguments that voluntary self-regulatory efforts are the best way to address privacy concerns in connection with behavioral targeting of children online. Strong legal requirements along with vigilant enforcement are needed to protect children from tracking and targeting on the Internet.

Children should be able to grow up in an electronic oasis that enables access to online education, to education and entertainment opportunities in a safe environment. And I look forward to working with you, Madam Chair, and all the members of the committee so that we can strengthen privacy safeguards and ensure that kids and teens are protected when they go online, and that is why I introduced the Do Not Track Kids Act.

Mr. Simpson, you mentioned in your testimony that teens still need privacy protection online because, as we know, COPPA covers users 12 and younger. I agree with you. And the Do Not Track Kids bill that Joe Barton and I introduced provides teens with safeguards specifically tailored for their age group without expanding the COPPA structure to adolescents. Can you expand on Common Sense's views on privacy protections for teens, please?

Mr. SIMPSON. Thank you, sir. We think you are taking very much the right approach. There is a complicated issue here called child development and we all know that not all 8-year-olds are the same, 8-year-olds are not the same as 14-year-old, and 14-year-olds are not the same as 20-year-olds, and many 20-year-olds act like 12-year-olds. But the reality is that teens need something more than they have right now. The FTC's recommendations are very valuable for kids under 13, but there are a lot of 13- and 14- and 15-year-olds who are quite capable of making mistakes in this innovative space, and those mistakes can come back to haunt them. They need opportunities and they need a lot more education and they need a lot more information that is actionable. They need resources they can use that are designed for their age group, not for the lawyers who are well versed in privacy.

Mr. MARKEY. Thank you.

Dr. Montgomery, do you agree that younger teens need a framework for them as well, perhaps not for the 12 and under but something tailored for that group?

Ms. MONTGOMERY. Yes, I do and this is something I have felt very strongly about for a long time since we were debating COPPA where the issue of whether we ought to apply the COPPA protections to teens was very much part of the discussion at that time. And what I really believe is that we do need protections here. What we have seen is with COPPA, we have a framework where there is an industry that appreciates the concerns about children, but with teenagers, it has been no holds barred and no real sensitivity to their concerns.

Mr. MARKEY. Can I ask, what is your response to the questions that are raised by the eraser button that Mr. Barton and I have included in our bill? What do you think about its functionality as a way for parents to be able to protect kids?

Ms. MONTGOMERY. I don't really know how the eraser button will work but I do believe, as my colleague Alan Simpson has said, that teenagers themselves should be able to have some control over the information they have placed online.

Mr. MARKEY. Mr. Simpson, what is your view in terms of the eraser button?

Mr. SIMPSON. Absolutely. And you know, we don't know exactly how they will work, but I think they key is here we have seen a lot of innovation on how to collect and not enough innovation on

how to protect. And I think something like an eraser button is a tool that industry can design to empower teens in richer ways.

Mr. MARKEY. OK. Thank you. And I thank all of you for your participation in this very, very important discussion. It is only going to get more and more dangerous for kids if we don't put these safeguards in place.

Thank you, Madam Chair.

Mrs. BONO MACK. Thank you, Mr. Markey.

And again, I would like to thank Ms. Engle and the entire staff at the FTC who has devoted time and thought to this effort. Job well done. And also to all of you once again, thank you. I would like to say that this is a third in our series of online privacy hearings so far this year. I look forward to our continued discussions on how we can best balance the need to remain innovative with the need to protect all of our privacy, certainly our children's privacy.

Next week, we will take a close look at consumer attitudes and expectations, and we know that is going to be a very interesting hearing.

I will remind members that they have 10 business days to submit questions for the record, and I ask all witnesses to please respond promptly to any questions you might receive.

And the hearing is now adjourned. Thank you again.

[Whereupon, at 11:02 a.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

U.S. House of Representatives
"Protecting Children's Privacy in an Electronic World"
Hearing October 5, 2011
FTC Responses to Questions for the Record

The Honorable Joe Barton

1. **If you do not expand protections of the law to 13-17 year olds specifically, how do you protect them in your opinion?**

   The FTC staff's December 2010 Privacy Report highlighted the need to ensure that companies adopt basic principles to improve consumer, including teen, privacy. The principles articulated in that staff report – building basic privacy protections into the development and operation of online services, providing simplified choice mechanisms for data collection and use practices that matter to consumers, and improving the transparency of data practices – will benefit all consumers, including teens who are heavy users of online services. In addition, the staff report sought comment on the extent to which teens warranted additional protections. For example, the 2010 staff report asked whether more limited default settings would be appropriate for teen users of social media services. Some commenters and policymakers also have suggested that teens be given the ability to delete content they no longer wish to be public. The FTC is evaluating this input and expects to issue a final staff report in the coming months.

2. **Mobile applications are explicitly covered in the Do Not Track Kids Act of 2011 introduced by Mr. Markey and myself. Is there a reason why you do not explicitly cover mobile applications in your new proposed changes to the Children's Online Privacy Protection Act?**

   As the Commission articulated in its Notice of Proposed Rulemaking proposing amendments to the COPPA Rule, we believe that both the COPPA statute and the Commission's Rule are written broadly enough to encompass many new technologies without the need for new statutory language. Specifically, the statutory term "online service" covers any service available over the Internet, or that connects to the Internet or a wide-area network. We believe this includes mobile applications that allow children to play network-connected games, engage in social networking activities, purchase goods or services online, receive behaviorally targeted advertisements, or interact with other content or services. For this reason, the Commission does not believe that the term "online service" needs to be further defined either in the statute or in the Rule. In fact, the Commission recently took action against a mobile app developer, W3 Innovations, for its alleged failure to comply with COPPA in connection with its collection of personal information through several child-directed mobile apps.

The Honorable Henry A. Waxman

The Commission's notice proposing to amend the COPPA rule contains a discussion regarding "COPPA Coverage of Emerging Technologies." (76 Fed. Reg. 59807). That discussion states that "the Commission does not believe the term "online service" needs to be further defined either in the statue or the rule." It goes on to say: "Although many mobile activities are online services, it is less clear whether *all* short message services ("SMS") and multimedia message services ("MMS") are covered by COPPA. (Emphasis added). In a footnote, the Commission concludes that "where mobile services do not traverse the Internet or a wide-area network, COPPA will not apply."

1. **Does this conclusion mean that phone-to-phone SMS and MMS text messages are not an "online service" covered by COPPA?**

   COPPA applies to the collection and disclosure of personal information by commercial websites and online service providers and is thus, as a matter of law, expressly limited to online Internet-based services. Like ordinary phone calls, pure phone-to-phone SMS and MMS text messages that traverse wireless service providers' networks and short message service centers – rather than the "Internet" as defined by the COPPA statute – cannot be considered "websites located on the Internet" or "online services" and therefore do not trigger COPPA's requirements. However, not all "texting" programs are exempt from COPPA's coverage. For instance, mobile applications that enable users to send text messages from their web-enabled devices without routing through a carrier-issued phone number constitute "online services" under the statute. Likewise, retailers' premium texting and coupon texting programs that register users online and send text messages from the Internet to users' mobile phone numbers are "online services."

2. **Are there any other mobile services that would not be covered by COPPA as a result of this conclusion?**

   Yes. Mobile services that do not send or receive information over the Internet are not "online services" under COPPA. This would include those mobile applications that reside wholly on a user's device and do not send or receive information over the Internet.

3. **Is the Commission aware of any collection of information from children under age 13 by businesses through phone-to-phone text messages or other mobile services not covered by COPPA?**

   The Commission staff is aware of instances in the past in which marketers have advertised directly to children, urging them to use their mobile devices to register for mobile downloads such as ring tones, screen savers, music, pictures, and to receive various marketing messages. In 2006 and 2007, the Children's Advertising Review Unit of the Council of Better Business Bureaus (CARU), one of the four self-regulatory

programs approved by the Commission as a COPPA safe harbor, brought a series of actions involving these practices. Some of these matters involved the collection of personal information from children via a website and thus were covered by COPPA; others, however, collected the child's mobile phone number via text messages and therefore were not covered by COPPA. The Commission believes that CARU's actions as well as best practices guidelines subsequently adopted by the mobile industry helped to curtail the collection of personal information from children in this fashion.

4. **If such collection is occurring or could occur on a significant scale, does the Commission believe the COPPA statute should be updated to cover these practices? Please explain why or why not.**

As indicated above, the Commission staff does not believe that the collection of information from children through phone-to-phone text messages or other mobile services is occurring on a significant scale. At the present time, the Commission does not have a sufficient record to determine whether the statute should be expanded to cover SMS text messaging or any other form of phone-to-phone communications. For this reason, the Commission does not recommend a statutory amendment at this time.

5. **If the Commission believes the statute should be updated to cover these practices, can you please provide legislative language or guidance to cover these practices and any other mass means of communicating with and collecting information from children without reference to the Internet or a wide area network that could emerge in the future?**

The Commission does not recommend any changes to the COPPA statute at this time.

To: The Subcommittee on Commerce, Manufacturing, and Trade
From: Stephen Balkam, CEO, Family Online Safety Institute
Re: Responses to Additional Questions for the Record from **The Honorable Joe Barton**

1. Who funds the Family Online Safety Institute? They also fund the internet and desire to collect information of consumers on the internet, correct?

The Family Online Safety Institute (FOSI) is an international non-profit with 25 members, that includes AOL, AT&T, BT Retail, Comcast, Disney, Entertainment Software Association, Facebook, France Telecom, Google, GSM Association, Microsoft, Motion Picture Association of America, NCTA, Nominum, Optenet, RuleSpace, Sprint, StreamShield, Symantec, Time Warner Cable, Telefónica, USTelecom, The Wireless Foundation, Verizon and Yahoo!.

Each member company is entitled to take a seat on the board of directors upon joining. The board is responsible for determining the overall direction of the organization. The one seat per company rule ensures that no individual company, nor sector of the Internet, has more influence over the work of the organization than the others. FOSI works with its members to promote best practices in the field of online safety and privacy within the industry as a whole as well as within individual companies.

FOSI receives funding from members, private trusts, and foundations as well as bringing in revenue through exhibitors and attendance fees from events such as the FOSI Annual Conference.

2. My understanding is that you do not support the Barton/Markey bill correct?

We appreciate the hard-work and attention to the important issues facing kids on the Internet by Congressmen Barton and Markey. However, as we outlined in our written and oral testimony, it is our opinion that the "Do Not Track Kids Act of 2011" presents both Constitutional and technological difficulties. One of our concerns is the lack of specifics over how the "Eraser Button" would be created and enforced.

Technology mandates have a history of unintended consequences and we have concerns about what may occur with this button. The concept of an "Eraser Button" also poses First Amendment concerns with regards to the press as well as seriously infringing upon the Court protected rights of teens. This could cause issues particularly for older teens who have some free expression rights and may already be living away from their parents at college and learning to make their own decisions about what content they post online. We do not believe that the Bill gives adequate considerations to the technical practicalities of such an idea. FOSI also believes that many of the FTC proposed revisions to the COPPA rule address the concerns outlined in the bill.

3. Do you oppose the use of supercookies in your group?

We encourage further investigation into the use of supercookies, and agree with Congressmen Barton and Markey that the Federal Trade Commission is best suited for this role. With all cookies and tracking devices we believe in education of consumers, clear choice and transparent practices by companies that make it easier for consumers to delete cookies. We share your concerns about supercookies and are learning more about these new practices.

400 7th Street, NW • Suite 306 • Washington, DC 20004, USA • Tel: (+1) 202 775 0131 • Fax: (+1) 202 737 0085 • www.fosi.org